Using Technician Interface Software

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114088 Rev. A
August 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988-1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Using Technician Interface Software

About This Guide

Audience xx
Before You Begin xx
Conventions xxi
Acronyms xxii
Ordering Bay Networks Publications xxv

Technical Support and Online Services

Bay Networks Customer Service xxviii
Bay Networks Information Services xxix
World Wide Web xxix
Customer Service FTP xxix
Support Source CD xxx
CompuServe xxx
InfoFACTS xxxi
How to Get Help xxxi

Chapter 1
Introducing the Technician Interface

Differences from Site Manager 1-2
Running the Technician Interface 1-3
Logging In 1-3
User/Manager Login 1-3
Login with Password 1-4
Login with SecurID 1-4
Technician Interface Welcome Screen 1-10
Login Timeout Guidelines 1-11
Login Configuration 1-12

Logging Out 1-12
Starting a Manager Session from within a User Session 1-13
Using Technician Interface Scripts 1-13

Chapter 2
Configuring the Console Port

Overview 2-2
Configuring Console Port Parameters 2-2
Using the list Command 2-2
Using the set Command 2-3
Using the commit Command 2-4
Using the save Command 2-4
Console Port Parameters 2-4
Using Autoscript Files 2-19
Sample Autoscript Files 2-20
Customizing Autoscript Files 2-21

Chapter 3
Using Operating Commands

Overview 3-1
Displaying Online Help 3-2
Pausing and Scrolling the Screen 3-2
Halting a Command 3-3
Repeating the Command Last Entered 3-3
Repeating a Command Recently Entered 3-4
Loading a Command into Memory 3-7
Pinging a Remote Device 3-7
IP Ping 3-8
IPX Ping 3-12
OSI Ping 3-15
VINES Ping 3-18
AppleTalk Ping 3-21
APPN Ping 3-24
Displaying the ATM ARP Table for an Interface 3-27

Chapter 4
Managing a NonVolatile File System

Overview 4-2
Using Multiple Memory Cards 4-3
Naming Files: Rules and Conventions 4-5
Displaying the Status of All Memory Cards 4-6
Displaying a Directory 4-7
Changing the Active Volume 4-10
Copying a File 4-11
Copying Files from NVFS to DOS 4-11
Transferring a File 4-13
In-Band File Transfers 4-14
Out-of-Band File Transfers 4-17
Displaying the Contents of a File 4-17
Deleting a File 4-18
Compacting File Space 4-19
Formatting a Memory Card 4-20
Transferring a File to a Full Memory Card 4-20
Partitioning a Memory Card or SIMM 4-21

Chapter 5
Managing a DOS File System

Overview 5-2
Naming Files and Directories 5-3
Mounting a Volume 5-4
Unmounting a Volume 5-6
Changing the Working Directory 5-7
Displaying a Directory 5-8
Labeling a Diskette 5-11
Creating a Directory 5-12
Removing a Directory 5-12
Renaming a File or Directory 5-13
Copying a File 5-14
Copying Files from DOS to NVFS 5-15
Transferring a File 5-15
In-Band File Transfers 5-16

Out-of-Band File Transfers 5-18
Changing File Attributes 5-19
Displaying the Contents of a File 5-20
Deleting a File 5-21

Chapter 6
Managing Events

Overview 6-2
Logging and Displaying Event Messages 6-2
Applying Write Filters to the Events Log 6-3
Displaying Active Write Filters 6-5
Applying Read (Display) Filters to the Events Log 6-6
Saving the Events Log 6-8
Saving the Events Log Automatically 6-10
Log Autosave Platform Differences 6-11
Configuring the Log Autosave Feature 6-12
Displaying an Events Log File Previously Saved 6-13
Clearing Events 6-14

Chapter 7
Accessing the MIB

Listing MIB Objects 7-2
Getting MIB Values 7-4
Setting MIB Values 7-6
Committing MIB Sets 7-8
Saving the Configuration 7-9
Using the MIB-II Counter 7-9

Chapter 8
System Administration

AN/ANH/ASN Administration 8-2
Configuring the Boot Source 8-3
Configuring Initial Interfaces and Netboot Operation 8-5
Configuring the Initial IP Synchronous Interface 8-5
Configuring an Ethernet Interface for Network Booting 8-7
Enabling and Disabling Interfaces with ifconfig 8-8
Booting the Router 8-9

How the Router Boots 8-9
Booting 8-10
Using the PCMCIA/Floppy Switch 8-12
Booting after Crossnet Shutdown Notification (BNX Only) 8-13
Configuring Delayed Boot Services 8-14
Adding Delayed Boot Services to a Router 8-14
Scheduling Delayed Boot Events 8-15
Managing Delayed Boot Services 8-20
Disabling or Re-enabling Delayed Boot Services on a Router 8-20
Disabling or Re-enabling a Delayed Boot Event 8-20
Modifying Attributes for Scheduled Delayed Boot Events 8-21
Deleting Delayed Boot Events 8-21
Deleting Delayed Boot Services from the Router 8-21
Restarting a Slot 8-22
Restarting After Crossnet Shutdown Notification (BNX Only) 8-23
Resetting a System or Slot 8-24
Resetting After Crossnet Shutdown Notification (BNX Only) 8-28
Running Diagnostics 8-29
Turning off the DIAG Indicator LED 8-32
Displaying the Software Version 8-32
Halting Packet Transfer between Slots 8-33
Verifying and Upgrading Software 8-33
Validating an Executable File 8-35
Upgrading and Verifying a PROM 8-38
Upgrading PROMs Remotely 8-39
Determining Current PROM Image Versions 8-39
Determining the Version of the Current Boot PROM Image 8-40
Determining the Version of the Current Diagnostics PROM Image 8-40
Using the prom Command 8-41
Viewing the Load Addresses and Sizes of Applications 8-44
Setting the ACE Backplane Type 8-46
Resetting the Date and Time 8-46
Assigning Passwords 8-48
Enabling and Disabling SecurID Authentication 8-50
Enabling SecurID Authentication 8-50

Disabling SecureID Authentication 8-52
Managing SNMP Secure Mode 8-52
Setting the Router to Operate in Secure Mode 8-53
Setting the Encryption Key 8-54
Resetting the Security Counter 8-54
Customizing Hardware Compression Search Depth 8-55
Testing Compression and Throughput 8-56
WCP Search Depth Attributes 8-57
Displaying a Greeting or Notice Before the Login Prompt 8-59
Customizing the Technician Interface Welcome Message 8-59
Recording Console Messages to a File 8-60
Enabling Internal Clocking Mode 8-62
Responding to QENET Underflow Errors 8-62
Monitoring ip Routes 8-63
Routing Tables 8-72
Interface Cache 8-73
Multicast Cache 8-74
Slot/Internal Cache 8-75
OSPF Link State Database 8-76
Determining Circuit Numbers 8-76
Technician Interface Commands and Access Levels 8-78

Chapter 9
Managing Aliases

Creating and Displaying an Alias 9-2
Inserting Parameters in an Alias 9-3
Inserting Character Strings in an Alias 9-5
Debugging Aliases 9-7
Deleting an Alias from Memory 9-7
Saving Aliases to a File 9-8
Loading Aliases from a File 9-9
Debugging with Predefined Aliases 9-10

Appendix A
Using the Bay Networks Router MIB

Overview A-2

Bay Networks Router MIB Files A-7
Compliance with Specifications A-7
Implementation Notes A-8
MIB-II Object Definitions A-8
Supported Traps A-9
Unsupported Operations A-10
Line Number Attributes A-10

Appendix B
Using Out-of-Band Access to Transfer Files

Overview B-1
About xmodem B-2
The xmodem Command B-4
Command Parameters B-5
Command Options B-5
Filenames B-7
For More Information B-7
Implementation Notes B-7
File Handling B-8
Error Checking B-8
Canceling a File Transfer B-8
Modem Interface Differences B-8
Viewing xmodem Log Events B-9
Hardware Configuration B-9
Out-of-Band File Transfers from a UNIX Workstation B-10
Opening a Connection B-10
Transferring Files from Router to UNIX Workstation B-10
Transferring Files from UNIX Workstation to Router B-13
Out-of-Band File Transfers from a Windows Workstation B-17
xmodem and the Bay Networks Communications Terminal Program B-17
Opening Wfterm B-18
Checking and Verifying Current Modem Interface Settings B-19
Initializing the Local Modem B-21
Using Wfterm Telephone Call Functions B-22
Dialing a Remote Router B-22
Logging In to the Router's Technician Interface B-24

File Transfer Functions B-24
Transferring Files from Router to DOS Workstation B-25
Transferring Files from DOS Workstation to Router B-28
Closing the Connection B-30
Quitting Wfterm B-31

Appendix C
Using Syslog Messaging to
Monitor Router Events

Overview C-1
Remote Hosts and Filters C-4
Polling the Events Log C-5
Identifying Entity Filters C-5
Filtering by Event Number C-6
Filtering by Event Severity Level C-7
Filtering by Slot Number C-7
Mapping Router Event Messages into Syslog Message Format C-8
IP Header C-9
UDP Header C-10
UDP Data C-10
Priority Code C-10
Time Sequencing Syslog Messages C-12
Syslog Message Handling (on a Workstation) C-12
Configuring Syslogd on a UNIX Workstation C-13
Configuring Syslog on the Router C-15
Task 1: Logging In to the Router's Technician Interface C-16
Task 2: Defining a Slot Mask for Syslog on the Router C-16
Task 3: Creating Syslog on the Router C-16
Task 4: Configuring Syslog Global Attributes C-16
Task 5: Adding a Remote Host to the Syslog Host Table C-17
Task 6: Adding an Entity Filter for a Remote Host C-18
Task 7: Adding More Hosts or Entity Filters C-22
Task 8: Saving Your Syslog Configuration on the Router C-22
Task 9. Log Out of the Technician Interface C-22
Managing Syslog on a Router C-23
Disabling or Re-enabling Syslog on the Router C-23

Disabling or Re-enabling Syslog Hosts or Filters C-24
Deleting Remote Hosts or Entity Filters from the Syslog Configuration C-25
Deleting Syslog from the Router C-25
Example Syslog Configuration C-26
Syslog Parameter Descriptions C-28
Global/Group Parameters C-30
Host Parameters C-33
Entity Filter Parameters C-37
For More Information C-47

Index

Figures

Figure 1-1. SecurID Login Procedure and Interface Dialog 1-8
Figure 1-2. SecurID PIN Assignment Procedure and Interface Dialog 1-9
Figure 1-3. Technician Interface Welcome Screen 1-10
Figure 4-1. Sample Dinfo Display 4-6
Figure 4-2. Sample NVFS Directory Listing 4-8
Figure 5-1. Mounting a Volume 5-5
Figure 5-2. Sample DOS Directory Listing 5-9
Figure 8-1. RUIBOOT Date and Time Entry 8-16
Figure 8-2. RUIBOOT Date and Time Example 8-18
Figure 8-3. Sample Response to readexe Command 8-36
Figure A-1. Sample Top-Level Hierarchy of the Bay Networks Router MIB A-3
Figure B-1. Modem Connection B-9
Figure B-2. Wfterm Icon B-18
Figure B-3. The Wfterm Base Program Window B-18
Figure B-4. Accessing the Modem Settings Window B-20
Figure B-5. Verifying or Modifying Modem Interface Settings B-20
Figure B-6. Verifying Successful Modem Initialization B-21
Figure B-7. Accessing Wfterm Telephone Call Functions B-22
Figure B-8. The Wfterm Dial Command WIndow B-23
Figure B-9. The Wfterm File Transfer Operation Selection Window B-25
Figure B-10. The Wfterm File to Transfer Window B-27
Figure B-11. The Wfterm Connection Closed Window B-30
Figure B-12. Exiting/Quitting the Wfterm Program B-31
Figure C-1. Syslog and Syslogd Operation C-3
Figure C-2. Router Event Message Filtering for One Host C-5
Figure C-3. Syslog Message Encapsulation C-9
Figure C-4. Syslog Message Composition C-10

Tables

Table 4-1. NVFS Commands 4-3
Table 4-2. Router Software Images 4-4
Table 5-1. DOS File Management Commands 5-3
Table 5-2. DOS File Attributes 5-11
Table 5-3. DOS File Attribute Hex Values 5-19
Table 8-1. bconfig Command Settings 8-3
Table 8-2. ifconfig Command Settings 8-6
Table 8-3. ifconfig Settings for an Ethernet Interface 8-7
Table 8-4. Technician Interface Access Levels 8-78
Table 9-1. Aliases for Debugging Network Problems 9-10
Table B-1. Xmodem Option Flags B-6
Table C-1. Syslogd Error Levels C-44

About This Guide

Use this guide if you are responsible for maintaining a Bay Networks™ router or BNX® platform using Bay Networks Technician Interface commands. The guide provides an overview of the Technician Interface and instructions on how to

- Log in and log out
- Configure console port parameters
- Use the Technician Interface operating commands
- Manage a nonvolatile file system and DOS file system
- Use the Technician Interface to manage events
- Configure, enable, use, and disable Secure ID user authentication for Telnet login to the Technician Interface
- Access the Bay Networks MIB
- Perform system administration tasks, such as booting the router, resetting a slot, and running diagnostics
- Manage aliases
- Use out-of-band access to transfer files
- Use the router's Syslog messaging capability to manage event messages on any UNIX-based network management workstation

Audience

Written for network managers and router technicians, this guide assumes that you have a working knowledge of TCP/IP networking, and some familiarity with network management principles concerning the MIB, SNMP, system event messaging, file system and configuration management. The guide also assumes a working knowledge of hardware elements commonly used in Bay Networks routers, for example PROMs, Flash memory cards, and network cables.

Note: In this guide, the term *system* refers to the router system software.

Before You Begin

Before using this guide to run Technician Interface commands on a router or BNX platform, you must

- Install the router or BNX platform
- Use one of the following methods to establish a connection to the router or BNX platform:
  - -- Connect the serial port of an ASCII terminal device (for example, a DEC VT100) directly to the console port of the router or BNX platform.
  - -- Connect the serial port of a workstation or PC directly to the console port of the router or BNX platform. (Run ASCII terminal emulation software on the workstation or PC.)
  - -- Dial in to the console port of the router or BNX platform from a workstation or PC running ASCII terminal emulation software. (This alternative requires one modem locally attached to your workstation or PC, and another modem locally attached to the console port of the router or BNX platform you want to access.)
  - -- Establish a Telnet (in-band) connection to the router or BNX platform.

Note: Before you can access the Technician Interface using Telnet, the router or BNX platform must have at least one assigned IP address. Although there is no limit to the number of Telnet connections that you can make to the Technician Interface, we recommend that you establish no more than one Telnet session per router or BNX platform.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ACE	Advanced Communications Engine
AFN	Access Feeder Node
ALN	Access Link Node
AN	Access Node
ANH	Access Node Hub
APING	APPN Ping
APPN	Advanced Peer-to-Peer Routing
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Access Stack Node
ASN.1	Abstract Syntax Notation
AT	AppleTalk Protocol
ATM	Asynchronous Transfer Mode
AURP	Appletalk Update-based Routing Protocol
BCN	Backbone Concentrator Node
BGP	Border Gateway Protocol
BLN	Backbone Link Node
BLN-2	Backbone Link Node (2 power supplies)
BOOTP	Bootstrap Protocol
CLNP	Connectionless Network Protocol
CN	Concentrator Node
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCM	Data Collection Module
DLCMI	Data Link Control Management Interface
DLSw	Data Link Switch
DOS	Disk Operating System
DRAM	Dynamic RAM
DSAP	Destination Service Access Point
DVMRP	Distance Vector Multicast Routing Protocol

EOF	End of File
EGP	Exterior Gateway Protocol
FAT	File Allocation Table
FDDI	Fiber Distributed Data Interface
FIFO	First In First Out
FRSW	Frame Relay Switch
FTP	File Transfer Protocol
FN	Feeder Node
FR	Frame Relay
FRE	Fast Routing Engine
GAME	Gate Access Management Entity
GMT	Greenwich Mean Time
HDLC	High-level Data Link Control
HSSI	High Speed Serial Interface
ICMP	Internet Control Message Protocol
IGMP	Internet Group Membership Protocol
IN	Integrated Node
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LED	Light Emitting Diode
LLC	Logical Link Control
LMI	Local Management Interface
LN	Link Node
LNM	LAN Network Manager
LSP	Link State Packet
MAC	Media Access Control
MCT1	Multichannel T1
MIB	Management Information Base
MOSY	Managed Object Syntax
NML	Native Mode LAN

NSAP	Network Service Access Point
NVFS	Non-Volatile File System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCMCIA	Personal Computer Memory Card International Association
PPP	Point-to-Point Protocol
PPX	Parallel Packet Express
PROM	Programmable Read-Only Memory
QENET	Quad Ethernet
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RIF	Routing Information Field
RFC	Request for Comment
SAP	Service Access Point
SDLC	Synchronous Data Link Control
SIMM	Single In-line Memory Module
SMDS	Switched Multimegabit Data Services
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol
SR	Source Routing
SRM-L	System Resources Link Module
STA	Statistics, Thresholds, and Alarms
SYSCON	System Controller board
SWS	Switched Services
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
TIP	Terminal Interface Program
TP	Transaction Program
VC	Virtual Circuit
VINES	Virtual Networking System
WAN	Wide Area Network
XB	Translation Bridge
XNS	Xerox Networking Systems

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Introducing the Technician Interface

The Technician Interface provides management access to a Bay Networks router by means of

- Telnet (inband) connection to the router
- Direct or dial (out-of-band) connection to the router's console port

You can use the Technician Interface to install a router, and to maintain or diagnose router operation.

In addition, you can use the Technician Interface to monitor and configure certain basic functionality in the Bay Networks router. Refer to *Using Technician Interface Scripts* and *Writing Technician Interface Scripts* for more information on performing these tasks.

This chapter describes

- Differences between the Technician Interface and Site Manager
- How to log in and out of the Technician Interface
- Technician Interface scripts (brief overview)

Differences from Site Manager

The Technician Interface running on the router, and the Site Manager application running on a PC or UNIX workstation, both manage the router software. The Technician Interface differs from Site Manager as follows:

- The Technician Interface resides in the router's operating system kernel and automatically loads when you boot the router. You do not need to install the Technician Interface software from a separate medium first; all you need is an ASCII terminal or Telnet connection to the router. Site Manager, however, resides on a workstation and runs independently of router software.
- You establish a Technician Interface session through the router's console port, using a local ASCII terminal or dialup connection. You establish a Site Manager session independently and establish a connection in-band over the network.
- The Technician Interface scripts let you display information about various protocols and network services and enable or disable protocols, circuits, lines, and services.
- The Technician Interface is a command-line interface; it assumes that you are a network manager who knows the Technician Interface command syntax, the MIB, and SNMP. (The Technician Interface does provide online help, however.)

  In contrast, Site Manager is menu driven: when you display screens and select options from Site Manager's pop-up menus, it automatically sends the appropriate SNMP commands to the router. Site Manager also provides help text.

Caution: The Technician Interface does not provide the consistency checking or verification that Site Manager's static configuration feature provides. Technician Interface users can set erroneous values, commit the values to memory, and save the values to configuration files, thereby possibly disrupting router functionality and network activity.

Running the Technician Interface

The Technician Interface software entity normally runs on one slot only, except as noted otherwise in the following table:

Router Model:	Technician Interface runs on:
AN®	Slot 1 only
ASN™	Slots 1 to 4, individually or simultaneously, depending on the number of ASN routers stacked and the setup of the back panel for each router
BN (BLN®, BLN-2, BCN®)	Slot 2
LN® or CN® with SYSCON-II Flash system controller	Any slot (one slot only)

If you reset the slot on which the Technician Interface is running, the Technician Interface resets to another available slot on a multislot system, or to the same slot on a single-slot system.

Logging In

When you access the Technician Interface via Telnet or console session, you encounter up to three levels of router access security:

- User/Manager Login (Telnet and console access)
- Password Authentication (Telnet and console access)
- SecurID Authentication (Telnet access only)

User/Manager Login

To access the Technician Interface on a Bay Networks router, you must enter one of the following commands at the Login prompt that appears in your Telnet or console display:

```
Login: User
```

or

```
Login: Manager
```

Note: You must press the return key after every Technician Interface command. Technician Interface commands and passwords are case-sensitive. Use upper- and lowercase as indicated.

The User login entry allows you to enter *read-only* commands. These only read information from the router.

The Manager login entry allows you to enter any Technician Interface commands. Certain commands read information from the router and/or write information to the router.

We recommend limiting Manager access to network managers and the Bay Networks Technical Response Center. The section "Technician Interface Commands and Access Levels" in Chapter 8 lists all of the Technician Interface commands and their associated access requirements.

Login with Password

If you enable password authentication on a router, you must also enter a password after the Password prompt that appears following your login entry.

`Login:` *<User | Manager>*

`Password:` *<password>*

New routers initially have no password login requirements. If your network administrator enables password access on a router, the Password prompt appears when you attempt a login to that router. We recommend password access to help establish access and data security for routers in your network. For instructions on how to enable or disable password authentication on a router, see "Assigning Passwords" in Chapter 8.

Login with SecurID

SecurID is a feature for barring unauthorized users from accessing the Technician Interface on a Bay Networks router through a Telnet session.

If you enable this feature on a router, you enter in addition to a login entry a SecurID PASSCODE™ after the Passcode prompt, as follows:

`Login:` *<User | Manager>*

`Password:` *<password>* (if enabled)

`Passcode`: *<passcode>*

If your SecurID administrator enables the SecurID client on a router you need to access, you see the Passcode prompt at login time. When you enter a valid PASSCODE, you receive Technician Interface login privileges to the router. You receive on your Telnet access screen the Technician Interface login prompt, $: (or whatever your network administrator selects for the Telnet login prompt).

Each User or Manager authorized to access a router configured with an active SecurID client must have an electronic SecurID card issued by Security Dynamics, Inc. Security Dynamics programs each card with a Personal Identification Number (PIN) to uniquely identify its prospective owner, then assigns the card for exclusive use by that person only.

If you do not have an assigned PIN, the SecurID client on the router also prompts you through a routine for PIN assignment. (The SecurID administrator for your network must first configure the ID system to allow you access to the PIN assignment feature.) The SecurID administrator can enable you either to select your own PIN, or to accept a system-generated PIN.

The SecurID card uses an internal algorithm to electronically generate temporary "card codes." Before allowing you access to the Technician Interface of a router, the SecurID client requires you to enter your PIN, followed by the current card code from your SecurID card.

The SecurID server on your network either

- Recognizes your PASSCODE and grants access to the router's Technician Interface
- Does not recognize your PASSCODE and denies access to the router's Technician Interface

Note: If the SecurID system denies you access to a router after four login attempts, the system then removes your PIN from the current list of valid SecurID users. To reactivate your SecurID PIN, you must request reactivation from the SecurID administrator of your network.

Newly installed routers initially do not require SecurID authentication for Technician Interface login privileges. (The network administrator must first enable the feature on the router.)

We recommend SecurID authentication for routers that require the highest level of protection from unauthorized Telnet access to the Technician Interface. To support Technician Interface login via SecurID, you must have a Security Dynamics SecurID ACE® server system installed on your IP network. Routers with the SecurID ACE client enabled communicate with the SecurID server during each user authentication sequence.

For more information about SecurID server systems, contact your Bay Networks sales representative.

SecurID Login and PIN Assignment Dialog

This section describes more fully the interface dialog you may encounter when attempting a login to a router configured with SecurID client software. Normally you can open a Technician Interface session as long as you enter a valid PASSCODE (your PIN, followed by the current card code). If you do not have a valid SecurID PIN when you attempt the login, you may receive another series of prompts for automated PIN assignment.

Note: The SecurID administrator for your network must first configure the SecurID system to allow you to receive a PIN through the SecurID client software on the router.

Figure 1-1 shows the complete authentication procedure and interface dialog you may encounter when attempting a login to a router configured with SecurID client software. Whenever you enter information that the SecurID client considers incorrect, you receive more prompts until you log in successfully, or until the SecurID client denies you further access to the router.

Figure 1-2 shows the complete new PIN assignment procedure and interface dialog you encounter during your initial login attempt, if you do not already have a valid assigned SecurID PIN.

To configure the SecurID client software on the router, refer to "Enabling and Disabling SecurID Authentication" in Chapter 8.

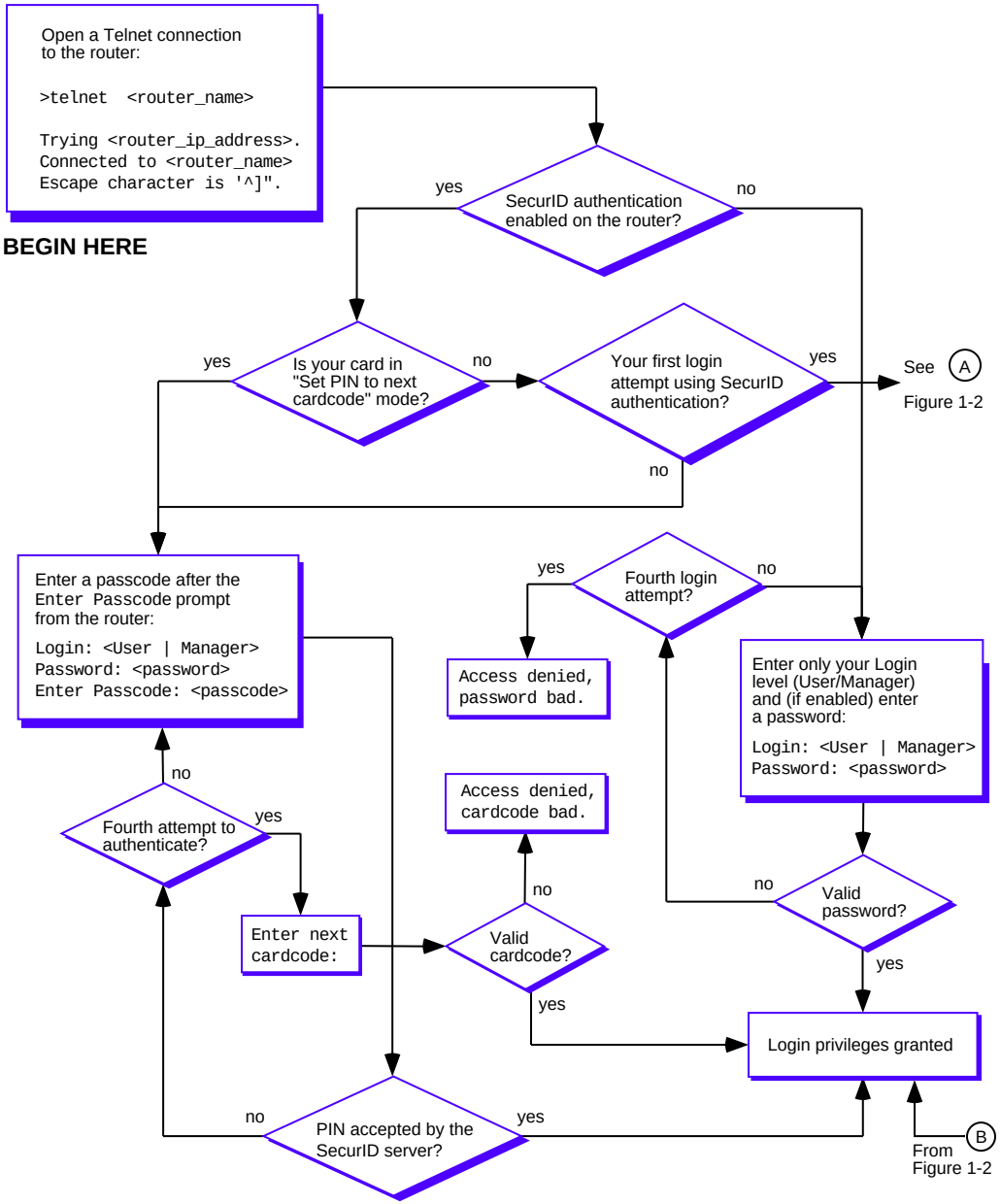


Figure 1-1. SecurID Login Procedure and Interface Dialog

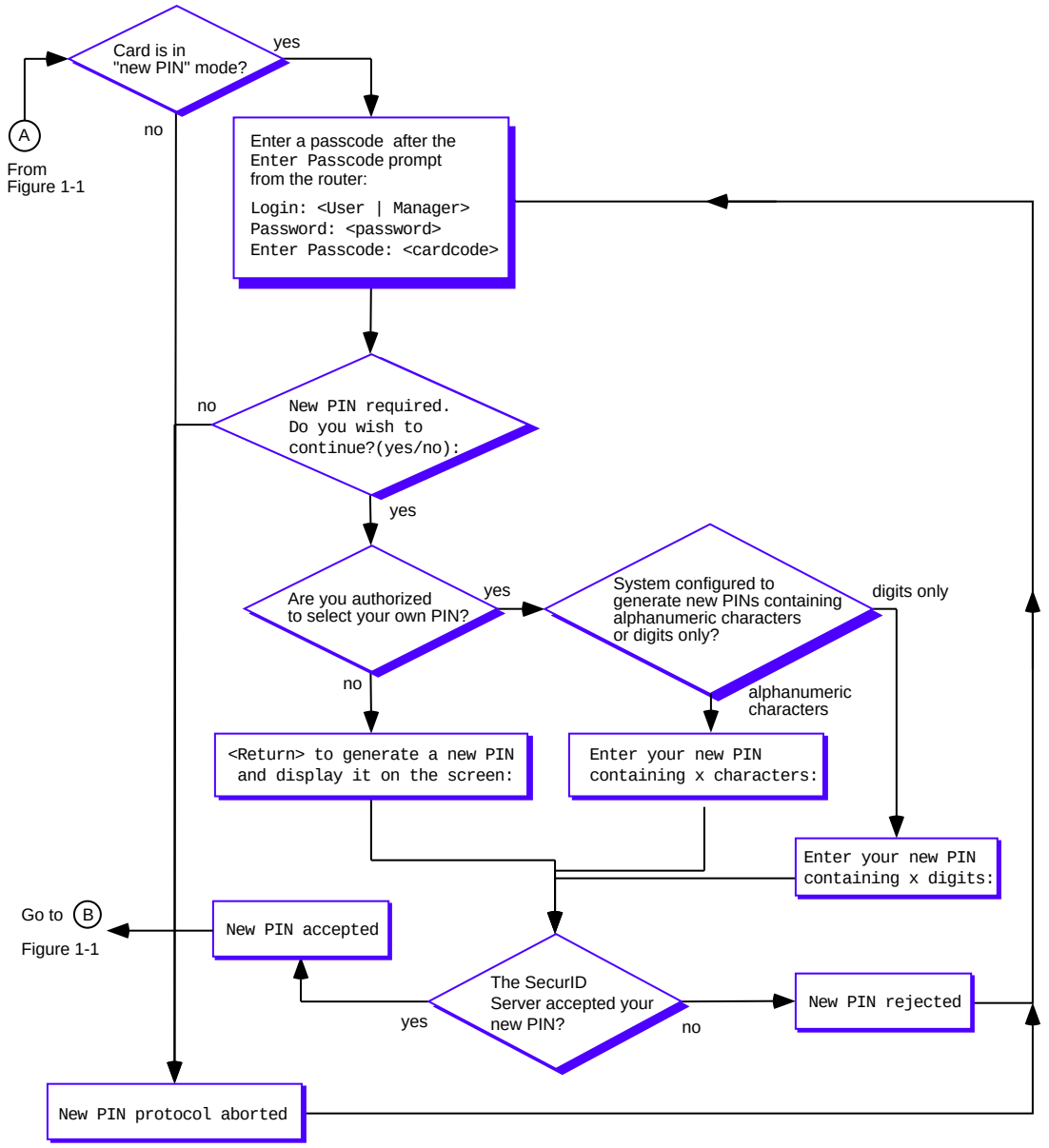


Figure 1-2. SecurID PIN Assignment Procedure and Interface Dialog

Technician Interface Welcome Screen

When you initially boot a router (during installation) using the configuration file *ti.cfg*, you receive a colon (:) as the login prompt on your console display or Telnet connection. For example, booting from a console locally connected to Serial Port 1 of a router initializes the Technician Interface on Slot 1 of that router, and you receive the prompt:

```
1:1
```

The “1” preceding the colon represents Slot 1, where the Technician Interface is running on the router.

The “1” following the colon represents Serial Port 1, where you physically connect the console or terminal to the router.

When you log into the system subsequently (by means of simple login, or with user authentication with password and/or SecurID), the Technician Interface by default displays a Welcome message and the $ prompt (Figure 1-3).

```
Bay Networks, Inc. and its Licensors.
Copyright 1992, 1993, 1994, 1995, 1996.
All rights reserved.



Login: Manager


      Welcome to the Backbone Technician Interface


$
```

Figure 1-3. Technician Interface Welcome Screen

Your network administrator can change the Technician Interface prompt you receive on a local or remote ASCII console or Telnet connection screen. For instructions on how to change the Technician Interface login prompt you receive on a local or remote ASCII terminal or console screen, see Chapter 2. For instructions on how to change the Technician Interface login prompt you receive on a remote Telnet screen, refer to the *Configuring TCP Services* guide.

You enter Technician Interface commands after the colon (:) prompt, the dollar sign ($) prompt, or whatever prompt your network administrator sets on the router for console or Telnet access to the router.

You can also customize the Technician Interface Welcome screen with a message appropriate for the requirements of your organization or network site. Refer to "Customizing the Technician Interface Welcome Message" in Chapter 8 for instructions.

Login Timeout Guidelines

Keep the following in mind when you enter your login name (**User** or **Manager**) and password:

- If you do not make an entry at the Login prompt for 1 minute (default), the Technician Interface disconnects from the router.
- If you do not make an entry at the Password prompt for 1 minute (default), the Technician Interface returns you to the Login prompt.
- If you enter the login name or password incorrectly 3 times (default), the Technician Interface disconnects you from the router.
- If you do not make an entry at the SecurID prompt for 1 minute (default), the Technician Interface returns you to the Login prompt.
- If you enter the SecurID PASSCODE incorrectly 4 times (default) the SecurID client software disconnects you from the router and initiates deactivation of your SecurID card account. (You must request reactivation from the SecurID administrator for your network.)

Login Configuration

For instructions on changing the default values associated with the console port, see "Configuring Console Port Parameters" in Chapter 2.

For instructions on changing the default values associated with Telnet access to the Technician Interface, refer to *Configuring IP Utilities*.

For information on changing the default values associated with SecurID services, see "Enabling and Disabling SecurID Authentication" in Chapter 8.

Logging Out

To exit a Technician Interface session, enter the following command after the Technician Interface prompt:

logout

For a console connected directly to the router, the Login prompt reappears:

`Login:` *<User | Manager>*

`Password:` *<password>* (if enabled)

`Passcode`: *<passcode>* (if enabled)

For a remote terminal program on a PC or workstation connected to the router by means of modems, the following messages appear, and the Technician Interface hangs up the telephone:

```
TI session logged out.

** Goodbye. **
```

Note: To use the Technician Interface with a modem, see Chapter 2.

If the Modem Enable parameter has a setting of Disable (default) and the session terminates unexpectedly, the router does not automatically log you out. You must re-establish a connection to the router and log out using the **logout** command.

Starting a Manager Session from within a User Session

You can initiate a Manager session within a User session by entering the following command:

system

The Password prompt appears at this time if your network administrator configured a password for Manager access. Enter the password after the prompt. The Technician Interface prompt appears when the system logs you in.

Enter **logout** to terminate the Manager session. You return to the User session when the Technician Interface prompt reappears.

Using Technician Interface Scripts

The Technician Interface scripts are programs that let you manage the router using information stored in the Management Information Base (MIB). You can use the scripts to display information about protocols and network services and to enable or disable protocols, circuits, lines, and services.

You access the Technician Interface scripts using the following commands:

- **show** displays system configuration, state, and statistical information. This command helps you isolate problems such as circuits that are not working, packets that are not being forwarded, and so on.
- **monitor** displays the same information as the **show** command but refreshes the display periodically so you can examine trends and changes.
- **enable**/**disable** enables or disables system features, protocols, drivers, or individual circuits.
- **menu** provides a menu interface to the other scripts. You can also use the menu-building features of this script to create custom menus.

A number of Technician Interface scripts exist as programs embedded within the router software image, rather than as individually loadable batch files (filename *<entity_name>.bat*). You run the embedded and batch file versions of scripts in an identical manner, using the script commands described in *Using Technician Interface Scripts*. The embedded scripts run more efficiently than scripts based on loadable batch files.

The router software currently includes embedded scripts for the following router software entities:

- CSMACD
- IP
- IPX
- FR
- FTP
- TCP
- TFTP
- SNMP
- SYNC
- TELNET

You can also use menus (described in *Using Technician Interface Scripts*) as an alternative way of accessing the full set of scripts.

Chapter 2
Configuring the Console Port

To configure a router's console port parameters using the Technician Interface, you have to change the default parameter settings associated with the console port on the back of the router. You can change the default parameter settings for the console port associated with the following boards:

- System Resources Link Module (SRM-L) board found in the BLN, BLN-2, and BCN routers
- System Input/Output (SYS I/O) board found in the FN®, LN, CN, and ALN routers
- Motherboard found in the AFN®, AN, and ASN routers

The autoscript feature allows you to automatically execute certain Technician Interface commands when you log in as either a Manager or User.

Note: You can use the console port to connect either a console or modem to the router.

Overview

You access the Technician Interface software through a console or modem attached to a router serial port. The number of Technician Interface sessions you can establish for a router depends on the number of serial ports available on that router.

- The SRM-L board has one serial port (labeled “Console”), allowing you to establish 1 session.
- The SYS I/O board has 3 serial ports (labeled “Console,” “Modem 1” and “Modem 2”), allowing you to establish up to 3 sessions.
- The AFN motherboard has two serial ports (labeled “Console” and “Modem”), allowing you to establish 1 or 2 sessions.
- The AN motherboard has 1 serial port (labeled “Console”), allowing you to establish 1 session.
- The ASN motherboard has one serial port per router, with up to 4 routers stacked, allowing you to establish up to 4 sessions with the interconnected stack.

Refer to *Configuring Routers* if you prefer to user Site Manager to configure the serial port parameters for the router console.

Configuring Console Port Parameters

The following sections describe how to use the following Technician Interface commands:

- **list**
- **set**
- **commit**
- **save**

Using the list Command

You can list and review all serial port attributes by entering the following command line at the Technician Interface prompt:

list wfSerialPortEntry

Using the set Command

Enter one of the following Technician Interface commands to configure a console port parameter:

set wfSerialPort Entry.*<attribute_name>.<port_no.> <option>*

set wfSerialPort Entry.*<attribute_no.>.<port_no.> <option>*

set	Refers to the Technician Interface **set** command. You must have Manager access to issue a **set** command.
wfSerialPortEntry	Refers to the MIB attribute name associated with all serial port parameters.
<attribute_name>	Is the MIB attribute name associated with one of the serial port parameters.
<attribute_no.>	Is the MIB attribute number associated with one of the serial port parameters.
<port_no.>	Is the number of the serial port you are configuring.
<option>	Is the new setting taken from the Options or Range list.

Example:

The following commands set the Parity parameter to Odd:

set wfSerialPortEntry.wfSerialPortParity.1 2

or

set wfSerialPortEntry.10.1 2

Note: You can use **s** instead of **set**.

Using the commit Command

Enter the following command after issuing one or more **set** commands:

commit

The **commit** command causes the changes you made to the configuration to take effect in active memory, but not in Flash memory. You must use the **save** command subsequently to save changes to a configuration file (*config*) and Flash volume on the router.

The Technician Interface software service resets when you enter the **commit** command.

Using the save Command

After you **set** and **commit** changes to the current configuration running in active memory on the router, use the **save** command to store that configuration to a file on a Flash memory volume, as follows:

save config *<vol>*:*<filename>*

Note: You can also use the **save** command to save the current contents of the router's Event log, environment variable list, or alias list. Refer to Chapters 6, 7, and 9 for more information on these applications of the **save** command.

Console Port Parameters

This section describes parameters for configuring the serial (console) port on the router:

- Parameter
- Attribute name
- Attribute number
- Bay Networks default setting
- Options or range of valid settings
- Parameter's function
- Instructions for setting the parameter
- Command you enter to configure or monitor the parameter

Note: You cannot configure the following console port parameters: State, Number, Name, and Slot.

Parameter:	**Port Delete**
Attribute Name:	wfSerialPortDelete
Attribute Number:	1
Default:	1 (Create)
Options:	1 (Create) | 2 (Delete)
Function:	Creates or deletes an instance of a console port.
Instructions:	Set to 1 (Create) to create a MIB record with system defaults for a console port. Set to 2 (Delete) to delete a MIB record for a console port.
Command:	**set wfSerialPortEntry.1.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.1

Parameter:	**Port Disable**
Attribute Name:	wfSerialPortDisable
Attribute Number:	2
Default:	1 (Enable)
Options:	1 (Enable) | 2 (Disable)
Function:	Enables or disables the console port.
Instructions:	Select the status of the console port.
Command:	**set wfSerialPortEntry.2.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.2

Parameter:	**Port State**
Attribute Name:	wfSerialPortState
Attribute Number:	3
Default:	4 (Not present)
Options:	1 (Up) | 2 (Down) | 3 (Init) | 4 (Not present)
	Up = enabled
	Down = disabled
	Init = initializing (for new instances)
	Not present = the port does not physically exist
Function:	Shows the current state of the port.
Instructions:	You cannot change this parameter.
Command:	**get wfSerialPortEntry.3.***<port_no.>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.3

Parameter:	**Port Number**
Attribute Name:	wfSerialPortNumber
Attribute Number:	4
Default:	None
Options:	1 | 2 | 3 | 4
Function:	The port number for the information being displayed. Not all routers have four physical ports. The system places a configured port that doesn't exist into the Not present state.
Instructions:	You cannot change this parameter.
Command:	**get wfSerialPortEntry.4.***<port_no.>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.4

Parameter:	**Port Name**
Attribute Name:	wfSerialPortName
Attribute Number:	5
Default:	None
Options:	Set by the system.
Function:	The name that the system has assigned to the port. Users may not specify a name. You can use this name to correlate the port number to the name printed on the hardware next to the physical port connection.
Instructions:	You cannot change this parameter.
Command:	**get wfSerialPortEntry.5.***<port_no.>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.5

Parameter:	**Port Slot**
Attribute Name:	wfSerialPortSlot
Attribute Number:	6
Default:	None
Options:	Set by the system.
Function:	The slot on which the login session for the console port is running. The system sets this number.
Instructions:	You cannot change this parameter.
Command:	**get wfSerialPortEntry.6.***<port_no.>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.6

Parameter:	**Port Type**
Attribute Name:	wfSerialPortType
Attribute Number:	7
Default:	1 (Technician Interface)
Options:	1 (Technician Interface) | 2 (Printer)
Function:	Configures the port for either Technician Interface (Console or Modem) or Printer. (The Printer option is not supported at this time.)
Instructions:	Set according to your console requirements.
Command:	**set wfSerialPortEntry.7.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.7

Parameter:	**Baud Rate**
Attribute Name:	wfSerialPortBaudRate
Attribute Number:	8
Default:	9600
Options:	9600 | 4800 | 1200 | 600 | 300
Function:	Specifies the rate of data transfer between the console and the router.
Instructions:	Set according to your console requirements.
Command:	**set wfSerialPortEntry.8.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.8

Parameter:	**Data Bits**
Attribute Name:	wfSerialPortDataBits
Attribute Number:	9
Default:	8
Options:	7 | 8
Function:	Specifies the number of bits in each ASCII character received or transmitted by the router.
Instructions:	Set according to your console requirements.
Command:	**set wfSerialPortEntry.9.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.9

Parameter:	**Port Parity**
Attribute Name:	wfSerialPortParity
Attribute Number:	10
Default:	1 (None)
Options:	1 (None) | 2 (Odd) | 3 (Even)
Function:	Enables or disables data error detection for each character transmitted or received.
Instructions:	Use the 2 (Odd) or 3 (Even) setting to enable data error detection. Use the 1 (None) setting to disable data error detection.
Command:	**set wfSerialPortEntry.10.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.10

Parameter:	**Stop Bits**
Attribute Name:	wfSerialPortStopBits
Attribute Number:	11
Default:	1 (1)
Options:	1 (1) | 2 (1.5) | 3 (2)
Function:	Specifies the number of bits that follow each ASCII character received or transmitted by the router. Selecting option 2 (1.5 stop bits) for any AN/ANH series router defaults to option 3 (2 stop bits).
Instructions:	Set according to your console requirements.
Command:	**set wfSerialPortEntry.11.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.11

Parameter:	**Modem Enable**
Attribute Name:	wfSerialPortModemEnable
Attribute Number:	12
Default:	2 (Disable)
Options:	1 (Enable) | 2 (Disable)
Function:	Specifies whether the terminal connects directly or via a modem to the Technician Interface.
Instructions:	Use the 1 (Enable) setting to configure the terminal for connection via a modem to the Technician Interface. Use the 2 (Disable) setting to configure the terminal for connection directly to the Technician Interface.
Command:	**set wfSerialPortEntry.12.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.12

Parameter:	**Lines Per Screen**
Attribute Name:	wfSerialPortLinesPerScreen
Attribute Number:	13
Default:	24 lines
Range:	1 to 512 lines
Function:	Specifies the maximum number of lines displayed on the console screen before the system displays the More prompt. The screen may override the number of lines you specify if Telnet can negotiate the window size with the remote client.
Instructions:	Set according to your console requirements.
Command:	**set wfSerialPortEntry.13.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.13

Parameter:	**More Enable**
Attribute Name:	wfSerialPortMoreEnable
Attribute Number:	14
Default:	1 (Enable)
Options:	1 (Enable) | 2 (Disable)
Function:	Specifies whether the Technician Interface pauses after each screen fills with data.
Instructions:	Select 1 (Enable) to configure the Technician Interface to pause after each screen fills with data. Select 2 (Disable) to configure the Technician Interface not to pause after each screen fills with data.
Command:	**set wfSerialPortEntry.14.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.14

Parameter:	**Prompt**
Attribute Name:	wfSerialPortPrompt
Attribute Number:	15
Default:	$
Options:	Any string of up to 19 keyboard characters except for control key sequences.
Function:	Specifies the character string used as the Login prompt on the Technician Interface console screen.
Instructions:	Accept the default ($) or specify a different character string. If you include spaces, enclose this string in quotes.
Command:	**set wfSerialPortEntry.15.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.15

Note: To help identify the slot where the Technician Interface (that is, your console or Telnet) session is running, you can configure the console and Telnet prompts on Bay Networks routers in your network to *<router_name>* [**%slot%**]. The router substitutes for "**%slot%**" the number of the actual slot where the session is running on the router. For more information on how to configure the Telnet prompt on a router, refer to *Configuring IP Utilities*.

Parameter:	**Login Timeout**
Attribute Name:	wfSerialPortLoginTimeOut
Attribute Number:	16
Default:	1 min
Range:	1 to 99 min (99 indicates infinity)
Function:	Specifies the number of minutes the Technician Interface waits to time out when no one has pressed the enter key after the Login prompt. This parameter is valid only when Modem Enable is set to 1 (Enable). The Technician Interface hangs up the phone when the timeout value is exceeded.
Instructions:	Accept the default (1 minute) or specify a different timeout value.
Command:	**set wfSerialPortEntry.16.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.16

Parameter:	**Password Timeout**
Attribute Name:	wfSerialPortPasswordTimeOut
Attribute Number:	17
Default:	1 min
Range:	1 to 99 min (99 indicates infinity)
Function:	Specifies the number of minutes the Technician Interface waits to time out when no one has pressed the enter key after the Password prompt. This parameter is valid only when Modem Enable is set to 1 (Enable). The Technician Interface returns to the Login prompt when the timeout value is exceeded.
Instructions:	Accept the default value (1 minute) or specify a different timeout value.
Command:	**set wfSerialPortEntry.17.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.17

Parameter:	**Command Timeout**
Attribute Name:	wfSerialPortCommandTimeOut
Attribute Number:	18
Default:	15 min
Range:	1 to 99 min (99 indicates infinity)
Function:	Specifies the number of minutes that can elapse before the Technician Interface disconnects the Telnet session, if you do not enter a command at the command prompt. This parameter is valid only when Modem Enable is set to 1 (Enable).
Instructions:	Accept the default value (15 minutes) or specify a different timeout value.
Command:	**set wfSerialPortEntry.18.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.18

Parameter:	**Login Retries**
Attribute Name:	wfSerialPortLoginRetries
Attribute Number:	19
Default:	3 login attempts
Range:	1 to 99 (99 indicates infinity)
Function:	Specifies the maximum number of login attempts you can make before the Technician Interface disconnects the Telnet session. This parameter is valid only when Modem Enable is set to 1 (Enable).
Instructions:	Accept the default value (3) or specify a different value.
Command:	**set wfSerialPortEntry.19.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.19

Parameter:	**Login Script Search Path**
Attribute Name:	wfSerialPortInitialSearchPath
Attribute Number:	28
Default:	2:
Range:	A string of valid volume numbers, depending on your login ID (Manager or User)
Function:	Specifies a list of file system volumes for the system to search if the manager's login script file or the user's login script file does not contain a volume specification. The environment variable PATH is set to this string.
Instructions:	Accept the default value (2:) to search for the Technician Interface autoscript files on Volume 2. Otherwise, enter a text string that uses the format: "<*vol*>: [;<*vol*>: ...]". For example, enter "A:;1:;2:" or "2:;4:;6:;9".
Command:	**set wfSerialPortEntry.28.***<port_no.>* **"***<option>***"**
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.28

Parameter:	**Manager's Login Script**
Attribute Name:	wfSerialPortManagerAutoScript
Attribute Number:	29
Default:	automgr.bat
Options:	The name of the manager's login script file.
Function:	Executes the manager's login script file automatically at login.
Instructions:	If you did not change the name of the manager's login script file, accept the default. Otherwise, enter the name of your manager's login script file. This name can have up to eight characters followed by up to a three-character extension. If the login script file does not contain a volume specification, the system searches the volumes you specify with the Login Script Search Path parameter.
Command:	**set wfSerialPortEntry.29.***<port_no.>* **"***<option>***"**
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.29

Parameter:	**User's Login Script**
Attribute Name:	wfSerialPortUserAutoScript
Attribute Number:	30
Default:	None
Options:	None or *autouser.bat*. A script named *autouser.bat* exists within the Technician Interface software. You can use the script as-is, or you can modify it to suit your requirements.
Function:	Executes the user's login script file automatically at login.
Instructions:	If you did not change the name of the user's login script file, accept the default. Otherwise, enter the name of your user's login script file. This name can have up to eight characters followed by up to a three-character extension. If the login script file does not contain a volume specification, the system searches the volumes you specify with the Login Script Search Path parameter.
Command:	**set wfSerialPortEntry.30.***<port_no.>* **"***<option>***"**
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.30

Parameter:	**Force User Logout**
Attribute Name:	wfSerialPortUserAbortLogoutDisable
Attribute Number:	31
Default:	2 (Disable)
Options:	1 (Enable) | 2 (Disable)
Function:	Specifies whether or not the user can execute a control-c (^C) to break out of a user autoscript at login (when a user autoscript is in effect).
Instructions:	Set the parameter to Enable to prevent the user from using ^C to break out of the user autoscript at login. Set the parameter to Disable to allow the user to execute ^C to break out of the user autoscript at login. Use the default (Disable) if you want users to access the Technician Interface. Set to Enable if you want to force users to enter the Telnet logout command.
Command:	**set wfSerialPortEntry.31.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.31

Parameter:	**History Depth**
Attribute Name:	wfSerialPortHistoryDepth
Attribute Number:	32
Default:	20 (commands)
Options:	1 to 40 (commands)
Function:	Specifies the maximum number of Technician Interface commands stored in the local command history table. The table stores each command you enter at the Technician Interface prompt on a first-in, first-out (FIFO) basis.
Instructions:	Set the maximum number of commands that you want the router to remember, for subsequent recall via the Technician Interface “history” command.
Command:	**set wfSerialPortHistoryDepth.32.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.32

Parameter:	**Maximum Autosaved Files**
Attribute Name:	wfSerialPortAutoSaveNumFiles
Attribute Number:	33
Default:	0 (log autosave off)
Options:	1 to 99
Function:	Specifies the number of times the system saves the events log to a new file automatically when the log is full. The system saves the log the maximum number of times you specify, or until the memory card or diskette drive on the router becomes full.
Instructions:	Accept the default value (0, disabled) or specify the number of times you want to save the log to a new file.
Command:	**set wfSerialPortEntry.33.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.33

Parameter:	**Autosave Volume**
Attribute Name:	wfSerialPortAutoSaveVolume
Attribute Number:	34
Default:	None
Options:	Any valid memory card volume (slot) number from 1 to 14 (or) the diskette drive designation, **-a**
Function:	Specifies the target volume where the system stores new log files saved through the log autosave feature.
Instructions:	Specify the memory card or diskette file system volume on which you want to save the events log through the log autosave feature.
Command:	**set wfSerialPortEntry.34.***<port_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.34

Using Autoscript Files

You can configure the Technician Interface to use the autoscript files *automgr.bat* and *autouser.bat*, so that the Technician Interface executes certain commands every time you log in as either a Manager or User.

To configure the Technician Interface to use these autoscript files, you must modify the following serial port parameters:

- Login Script Search Path
- Manager's Login Script
- User's Login Script
- Force User Logout

Use the Login Script Search Path parameter to specify the list of file system volumes to be searched. You can set up separate autoscript files to be run for the Manager login and the User login by configuring the Manager's Login Script and User's Login Script parameters. You can set the Force User Logout parameter when the User autoscript is in effect. This parameter locks the user into the User autoscript. When this parameter is enabled, any attempt to abort the script results in the user being logged out.

The Technician Interface configuration file, *ti.cfg*, looks for the *automgr.bat* script when the Manager logs in, or for the *autouser.bat* script when the User logs in. If the autoscript is not present, login proceeds normally without any error messages. The *ti.cfg* file has a default search path of slots 1 to 14 and a volume A. This works for any platform.

Sample Autoscript Files

The following autoscript files for the Manager login and the User login are configured using the Technician Interface software:

Manager login autoscript:

```
##############################################################################
#
#             Autoscript for Manager
#             Copyright 1995 Bay Networks Inc.
##############################################################################

#
#             Initialize aliases for script based commands
#
              alias sho“run show.bat  \$”
              alias show“run show.bat  \$”
              alias setpath“run setpath.bat  \$”
              alias disable“run disable.bat  \$”
              alias enable“run enable.bat  \$”
              alias monitor“run monitor.bat  \$”
              alias menu“run menu.bat  \$”
```

User login autoscript:

```
##############################################################################
#
#             Autoscript for User
#             Copyright 1995 Bay Networks Inc.
##############################################################################

#
#             Initialize aliases for script based commands
#

              alias sho“run show.bat  \$”
              alias show“run show.bat  \$”
              alias setpath“run setpath.bat  \$”
              alias disable“run disable.bat  \$”
              alias enable“run enable.bat  \$”
              alias monitor“run monitor.bat  \$”
              alias menu“run menu.bat  \$”
```

Customizing Autoscript Files

You can customize the *automgr.bat* or *autouser.bat* scripts by entering the appropriate commands or aliases into the scripts. Refer to Chapter 9 of this guide and the *Writing Technician Interface Scripts* guide for information on aliases and script files. Use **vi** or another text editor to edit *automgr.bat* or *autouser.bat* on your workstation. Then transfer the files via TFTP or XMODEM to the router where the scripts are located.

For instructions on using TFTP on a non-volatile file system, see Chapter 4. For instructions on using TFTP on a DOS file system, see Chapter 5. For instructions on using XMODEM, see Appendix B.

Chapter 3
Using Operating Commands

The basic Technician Interface operating commands allow you to

- Display online help
- Pause and scroll text on a screen
- Abort a command
- Repeat the command last entered
- Repeat a command recently entered
- Load a command into memory
- Ping a remote IP, IPX, OSI, VINES, AppleTalk, or APPN address
- Display the ATM ARP table for a specific IP interface address

Overview

Technician Interface commands, passwords, and filenames are case sensitive. You must press the return key to issue a Technician Interface command.

If you issue a command using an incorrect syntax, the Technician Interface displays the term *usage:* and the correct syntax to help you.

Refer to "Conventions" in the preface for conventions used in this documentation and the Technician Interface online help for information on Technician Interface commands.

Displaying Online Help

Use the **help** command to display online help text for any Technician Interface command, as follows:

help [<*command*>]

When you enter **help**, followed by a space and the name of a command, the console displays a detailed description of the command along with its syntax requirements. For example, when you enter **help date**, the console displays a detailed description of the **date** command.

To display all Technician Interface commands in a brief table, enter

help help

To display all Technician Interface commands and their associated syntax requirements, enter

help

Use this command as an online quick-reference card when you know the command's function, but don't know the command name or its syntax. The screen may scroll automatically; refer to the next section to control scrolling.

Pausing and Scrolling the Screen

Use the **more** command to view output before it scrolls out of view.

If the more mode is on, the system forwards the number of lines you specify to the screen and displays the following prompt at the bottom of the screen:

```
Type: <space> to page; <return> advance 1 line; Q to quit
```

If the more mode is off, the screen automatically scrolls when it fills.

Enter the following command to set or display the more mode:

more [**-s**] [**on** | **off**] *<#_of_lines>*

-s	Prevents the console from displaying output
on	Enables the more mode
off	Disables the more mode

Examples:

If you enter:	**The system:**
more	Displays more mode on or more mode off.
more on	Enables the more mode; pauses the system and prompts you to continue when a screen fills.
more -s on 24	Enables the more mode; sets screen size to 24 lines; no output displayed.
more on *<no.>*	Displays the number of lines that you specify before pausing.
more off	Disables the more mode. The screen scrolls automatically without prompting you.

Halting a Command

Press control-c (hold down the control key and press c) to halt processing of a command you just issued. This escape sequence returns Technician Interface prompt to your console or Telnet screen.

Repeating the Command Last Entered

Use the **repeat** command (**!**) to repeat execution of the last command you entered. You can specify an optional repetition count to repeat the command.

Enter the following to execute the last command you entered, where *<repeat_count>* is the optional number of times you want to execute the command. (The default is 1 time.)

! [*<repeat_count>*]

Examples:

If you enter:	The system:
!	Executes the last command you entered.
! 5	Executes the last command you entered five times.

Repeating a Command Recently Entered

Use the **history** command to

- View a list of the Technician Interface commands most recently entered during the current console or Telnet session.
- Recall and run a specific command from the history list.

The router retrieves the list from the command history table.

The history list contains up to 20 commands by default. You can increase the number of commands in the history list to a maximum of 40 by setting new values for the console (serial port) attribute wfSerialPortHistoryDepth, and the Telnet attribute wfTelnetHistoryDepth.

Example:

From a Technician Interface session:

%: set wfSerialPortEntry.wfSerialPortHistoryDepth = 40

%: set wfTelnet.wfTelnetHistoryDepth = 40

%: commit

By running the **history** command, you can recall and run any one of the last 40 commands you entered at the Technician Interface prompt.

Example:

$> **dinfo** *(Command 1)*

```
VOL    STATE      TOTAL SIZE    FREE SPACE    CONTIG FREE SPACE
-------------------------------------------------------------
 2:    FORMATTED    4194304        745101           697153
 4:    FORMATTED    4194304       2106021          2106021
```

$> **dir 2:** *(Command 2)*

```
 Volume in drive 2: is
 Directory of 2:

File Name             Size    Date     Day      Time
-----------------------------------------------------
bn.exe             3271441  06/12/95  Mon.    16:35:07
debug.al             12568  06/12/95  Mon.    16:38:57
install.bat         152524  06/12/95  Mon.    16:39:00
ti.cfg                 128  06/12/95  Mon.    16:39:08
mk_foo.cfg            4516  06/14/95  Wed.    14:18:39
config                2044  06/18/95  Sun.    13:57:35
syslog.cfg            2628  06/18/95  Sun.    15:58:09
osi.cfg               3048  07/19/95  Wed.    16:55:40

 4194304 bytes - Total size
  745101 bytes - Available free space
  697153 bytes - Contiguous free space
```

$> **stamp** *(Command 3)*

```
Image:     beta/9.00/1
Created:   Tue Jun 6 13:08:17 EDT 1995
```

$> **history** *(Displays the history list)*

```
    1  dinfo
    2  dir 2:
    3  stamp
```

$> **history 2** *(Repeats the second command currently in the history list)*

```
dir 2:

 Volume in drive 2: is
 Directory of 2:

File Name             Size    Date     Day      Time
-------------------------------------------------------
bn.exe             3271441  06/12/95  Mon.    16:35:07
debug.al             12568  06/12/95  Mon.    16:38:57
install.bat         152524  06/12/95  Mon.    16:39:00
ti.cfg                 128  06/12/95  Mon.    16:39:08
mk_foo.cfg            4516  06/14/95  Wed.    14:18:39
config                2044  06/18/95  Sun.    13:57:35
syslog.cfg            2628  06/18/95  Sun.    15:58:09
osi.cfg               3048  07/19/95  Wed.    16:55:40
```

Loading a Command into Memory

Use the **exec** command to load or unload dynamically loadable Technician Interface commands to and from memory.

Currently, you can load only the **telnet** command into memory. The **exec telnet** command is useful when booting a Bay Networks router over a network using BOOTP. Using **exec telnet** locks the **telnet** command into memory, in case the connection to the BOOTP server fails.

Enter the following to load a command into memory or unload a command from memory:

exec [-**load** | -**unload**] *<command_name>*

Once you load a command into memory, it remains there until you issue an **exec -unload** command, or until you restart the Technician Interface.

Pinging a Remote Device

Use the **ping** command to test the reachability of a remote device running the IP, IPX, OSI, VINES, AppleTalk, or APPN protocol. Although we use the term "ping" to refer to the action of testing the reachability of a remote device, our implementation of ping is different for each protocol. The following sections describe

- The procedure the router uses to ping a remote device running a given protocol
- The syntax of the **ping** command for each protocol
- The possible messages displayed when you issue the **ping** command

Note: The **ping** command is not case sensitive.

IP Ping

When you issue the **ping** command for IP, the ping program sends an Internet Control Message Protocol (ICMP) echo request to the remote IP address you specify. The remote device responds if it can be reached, and the console displays the response or the result of the request.

Enter the following to ping a remote device running IP:

ping -ip *<IP_address>* [**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*] [**-p**] [**-a***<address>*] [**-v**]

<IP_address> is the required IP address, in dotted decimal notation, of the remote device.

[**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*] [**-p**] [**-a***<address>*] [**-v**] are optional. These parameters are as follows:

<timeout> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 5.

<repeat_count> is the number of ping messages to send. Enter a value between 0 and 10 (inclusive). The default is 1.

<size> is the number of bytes of data to send with each ping. The default is 16.

-p generates a path trace report that displays the intervening hop addresses to the destination.

<address> is the source address.

-v (verbose) generates statistical information about the ICMP echo request, including information about the success rate and round-trip time.

Note: Our implementation of the ICMP protocol does not support loopback (pinging your own system) or broadcast addresses.

The console displays one of the following messages when you issue a **ping** command (if you enter a value in the <*repeat_count*> argument, the system displays one of the following messages for the default ping, plus one for each additional ping):

- An alive message: This message appears if the system receives an ICMP echo response from the target device within the <*timeout*> allowed. The message also indicates the size of the test packet. A sample message follows:

  ```
  ping: 192.32.1.151 is alive (size = 16 bytes)
  ```

- A does not respond message: This message appears if the system does *not* receive an ICMP echo response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  ping: 193.32.1.151 does not respond
  ```

- An ICMP host unreachable from y.y.y.y message: This message appears if the local Bay Networks router or remote router whose address is *y.y.y.y* cannot forward the ping request any further along the path to the target device. A sample message follows, where *y.y.y.y* is the address of the ICMP host:

  ```
  ping: ICMP host unreachable from 192.32.243.1
  ```

- A target address is unreachable message: The local Bay Networks router previously issued an ICMP host unreachable from y.y.y.y message. Within 40 seconds, the local Bay Networks router received a subsequent ICMP echo request addressed to the same target device. The ARP timed out or the address could not be resolved. A sample message follows:

  ```
  ping: 192.32.1.151 is unreachable
  ```

Examples:

If you enter (on one line):	The system:

ping -ip 192.32.1.151	Pings the device at the IP address 192.32.1.151 and waits up to 5 seconds (default) for a response. The console displays one of the following messages:
	`ping: 192.32.1.151 is alive (size = 16 bytes)`
	`ping: 193.32.1.151 does not respond`
	`ping: ICMP host unreachable from 192.32.243.1`
	`ping: 192.32.1.151 is unreachable`

ping -ip 192.32.1.151 -p	All of the above, but displays the intervening hop addresses to the destination before displaying the response message for each ping. For example, the console displays the following messages:
	`ping: (192.32.243.1)`
	`ping: (192.32.244.2)`
	`ping: 192.32.1.151 is alive (size = 16 bytes)`

If you enter (on one line):	The system:

ping 192.32.1.151 -t3 -r8 -s62	Pings the device at the IP address 192.32.1.151 eight successive times, sends 62 bytes of data with each ping, and waits up to 3 seconds for a response to each ping. The console displays one of the following for each ping sent:
	`ping: 192.32.1.151 is alive (size = 62 bytes)`
	`ping: 193.32.1.151 does not respond`
	`ping: ICMP host unreachable from 192.32.243.1`
	`ping: 192.32.1.151 is unreachable`

ping 192.32.1.151 -v	Provides statistical information about the ping of IP address 192.32.1.151. For example, the console displays the following messages:
	`(192.32.1.151): icmp_seq=0, time= 1 ms`
	`IP ping: 192.32.1.151 is alive (size = 16 bytes)`
	`---- PING Statistics----`
	`IP ping: 192.32.1.151 responded to 1 out of 1: 100% success.`
	`round-trip (ms) min/avg/max = 1/1/1`

IPX Ping

When you issue the **ping** command for IPX, the router sends an IPX configuration request packet to the remote IPX address that you specify. If the remote device is listening on socket number 456h for an IPX configuration request packet, it responds if it can be reached, and the console displays a message indicating that the device `is alive` or `does not respond.`

Note: The router also listens for, and responds to, the NLSP-based ping. However, NLSP-based ping is not currently an option of the **ping -ipx** command on the router.

IPX configuration request packets typically obtain configuration information from other devices on a NetWare network. However, the router only uses these packets to test the reachability of a remote device that listens for and responds to IPX configuration request packets.

Note: The Bay Networks IPX router will neither send nor acknowledge IPX configuration request packets addressed to network 0x00000000 (local network destination) or network 0xFFFFFFFF, or host 0x000000000000 or host 0xFFFFFFFFFFFF (broadcast host destination). The IPX router responds only to request packets sent directly to one of its interface addresses.

If you send a request packet from a router to an IPX interface on that same router, the router does not send the request packet out onto the line. Instead, the router sends the packet internally to the specified interface, which then responds internally.

Enter the following to ping a remote device running IPX:

ping -ipx *<IPX_address>* [**-t***<timeout>*] [**-r***<repeat_count>*]

<IPX_address> is the required IPX address, in hexadecimal or decimal notation, of the remote device.

An IPX address in hexadecimal notation consists of a 4-byte network address and a 6-byte host address, separated by a period (for example, 0x0000AB12.0x000000CD1234 [leading zero padding is not required]). The *0x* indicates that the address is in hexadecimal notation.

An IPX address in decimal notation consists of a 4-byte network address and a 6-byte host address, where

- Each byte is a number between 0 and 255, inclusive.
- A period separates successive address bytes (for example, 0.1.23.47.0.0.0.1.2.55).

Note: If you issue an IPX ping to an entity on a Token Ring network, you must enter the host portion of the IPX address in byte-swapped form (noncanonical form).

[**-t**<*timeout*>] [**-r**<*repeat_count*>] are optional. These parameters are as follows:

<*timeout*> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 5.

<*repeat_count*> is the number of ping messages to send. The system does not wait for the timeout before sending the next ping. Enter a value between 0 and 10 (inclusive). The default is 1.

The console displays one of the following messages when you issue a **ping -ipx** command. (If you enter a value other than 0 in the <*repeat_count*> argument, the system displays one of the following messages for the default ping, plus one for each additional ping):

- An `alive` message: This message appears if the system receives an IPX reply packet from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  IPX ping: 0xAB12.0xCD1234 is alive
  ```

- A `does not respond` message: This message appears if the IPX address of the target device is resolved, but the system does *not* receive an IPX reply packet from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  IPX ping: 0xAB12.0xCD1234 does not respond
  ```

- A `target address is unreachable` message: This message appears if the local Bay Networks router cannot find the specified network address in its table of IPX networks.

  ```
  IPX ping: 0xAB12.0xCD1234 is unreachable
  ```

- An `invalid parameter specified` message: This message appears if the network or host address is all 0s, all Fs, or not a valid IPX address. A sample message follows:

  ```
  IPX ping: invalid parameter specified
  ```

- A `resource error` message: This message appears if the router cannot allocate a buffer for the request because none are available. A sample message follows:

  ```
  IPX ping: resource error
  ```

Examples:

If you enter (on one line):	The system:

ping -ipx 0xAB12.0xCD1234	Pings the device at the IPX address 0xAB12.0xCD1234 and waits up to 5 seconds (default) for a response. The console displays one of the following messages:
	`IPX ping: 0xAB12.0xCD1234 is alive`
	`IPX ping: 0xAB12.0xCD1234 does not respond`
	`IPX ping: 0xAB12.0xCD1234 is unreachable`

ping -ipx 0xAB12.0xCD1234 -t3 -r8	Pings the device at the IPX address 0xAB12.0xCD1234 eight successive times and waits up to 3 seconds for a response to each ping. The console displays one of the following for each ping sent:
	`IPX ping: 0xAB12.0xCD1234 is alive`
	`IPX ping: 0xAB12.0xCD1234 does not respond`
	`IPX ping: 0xAB12.0xCD1234 is unreachable`
	The console also displays the following type of message after reporting the progress of each ping:
	`IPX ping: 0xAB12.0xCD1234 responded to 8 out of 8: 100% success`

OSI Ping

When you issue the **ping** command for OSI, the router sends a Connectionless Network Protocol (CLNP) echo request to the remote Network Service Access Point (NSAP) address you specify. The remote device responds with a CLNP echo response if it can be reached, and the console displays the response or the result of the request.

Enter the following to ping a remote device running OSI:

ping -osi <*NSAP_address*> [**-t**<*timeout*>] [**-r**<*repeat_count*>]

<*NSAP_address*> is the required NSAP address, in hexadecimal notation (0-9, A-F), of the remote device. (A leading 0*x* is not required when entering the NSAP address.)

[**-t**<*timeout*>] [**-r**<*repeat_count*>] are optional. These parameters are as follows:

<*timeout*> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 5.

<*repeat_count*> is the number of ping messages to send. The system does not wait for the timeout before sending the next ping. Enter a value between 0 and 10 (inclusive). The default is 1.

The console displays one of the following messages when you issue a **ping -osi** command. (If you enter a value other than 0 in the <*repeat_count*> argument, the system displays one of the following messages for the default ping, plus one for each additional ping):

- An `alive` message: This message appears if the system receives a CLNP echo response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  OSI ping: 49000400000a12121200 is alive
  ```

- A `does not respond` message: This message appears if the NSAP address of the target device is resolved, but the system does *not* receive a CLNP echo response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  OSI ping: 49000400000a12121200 does not respond
  ```

- A `<target address> is unreachable` message: This message appears if the local Bay Networks router cannot find the specified address in its routing table.

  ```
  OSI ping: 49000400000a12121200 is unreachable
  ```

- An `NSAP address is too short` message: This message appears if the NSAP address is too short. The minimum allowed NSAP address length is 20 hexadecimal characters (10 bytes). A sample message follows:

  ```
  OSI ping: NSAP address is too short
  ```

- An `OSI service is not running` message: This message appears if the OSI service is not enabled on the router. A sample message follows:

  ```
  OSI ping: OSI service is not running
  ```

- A `resource error` message: This message appears if the router cannot allocate a buffer for the request because none is available. A sample message follows:

  ```
  OSI ping: resource error
  ```

- A `system error` message: The message appears if the Technician Interface has failed. A sample message follows:

  ```
  OSI ping: system error
  ```

- A `<y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y.y> is a bad NSAP address` message: The message appears if the NSAP address is more than 20 hexadecimal characters or contains nonhexadecimal characters. A sample message follows.

  ```
  OSI ping: 4900040000a1121212000 is a bad NSAP address
  ```

Examples:

If you enter (on one line):	The system:

ping -osi 49000400000a12121200	Pings the device at the NSAP address 49000400000a12121200 and waits up to 5 (default) seconds for a response. The console displays one of the following messages:
	`OSI ping: 49000400000a12121200 is alive`
	`OSI ping: 49000400000a12121200 does not respond`
	`OSI ping: 49000400000a12121200 is unreachable`

ping -osi 49000400000a12121200 -t3 -r8	Pings the device at the NSAP address 49000400000a12121200 eight successive times and waits up to 3 seconds for a response to each ping. The console displays one of the following for each ping sent:
	`OSI ping: 49000400000a12121200 is alive`
	`OSI ping: 49000400000a12121200 does not respond`
	`OSI ping: 49000400000a12121200 is unreachable`
	The console also displays the following type of message after reporting the progress of each ping:
	`OSI ping: 49000400000a12121200 responded to 8 out of 8: 100% success`

VINES Ping

When you issue the **ping** command for VINES to a remote VINES device, it responds if it can be reached, and the console displays the response or the result of the request.

Enter the following to ping a remote device running VINES:

ping -vines *<network_address>.<host_address>* [**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*] [**-p**]

<network_address>.<host_address> is the required VINES address of the remote device. This address consists of a 32-bit serial number identifying the server node and a 16-bit subnetwork number identifying the node within the server node's logical grouping.

Note: You can enter the network and host addresses in decimal or hexadecimal format. If you use hexadecimal format, precede each address with the 0x prefix.

[**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*] [**-p**] are optional. These parameters are as follows:

<timeout> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 5.

<repeat_count> is the number of ping messages to send. The system does not wait for the timeout before sending the next ping. Enter a value between 0 and 10 (inclusive). The default is 1.

<size> is the number of bytes of data to send with each ping. The default is 16.

-p generates a path trace report that displays the intervening hop addresses to the destination.

Note: If you use the **-p** option to display the intervening hops to the destination, and the intervening hops are Bay Networks routers, the Technician Interface displays their network addresses. Otherwise, it displays a *.* for each hop that is not a Bay Networks router.

The console displays one of the following messages when you issue a **ping** command (if you enter a value in the <*repeat_count*> argument, the system displays one of the following messages for the default ping, plus one for each additional ping):

- An `alive` message: This message appears if the system receives a response from the target device within the <*timeout*> allowed. The message also indicates the size of the test packet. A sample message follows:

  ```
  VINES ping: 2705682.8003 is alive (size = 16 bytes)
  ```

- A `does not respond` message: This message appears if the address of the target device is resolved, but the system does *not* receive a response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  VINES ping: 2705682.8003 does not respond
  ```

- A *<target address>* `is unreachable` message: This message appears if the local Bay Networks router cannot find the specified address in its routing table. A sample message follows:

  ```
  VINES ping: 2705682.8003 is unreachable
  ```

- An `invalid parameter specified` message: This message appears if you specify an invalid parameter when you issue a **ping -vines** command. A sample message follows:

  ```
  VINES ping: invalid parameter specified
  ```

- A `resource error` message: This message appears if the local Bay Networks router cannot allocate a buffer for the request because none is available. A sample message follows:

  ```
  VINES ping: resource error
  ```

- A `VINES service is not running` message: This message appears if the VINES service is not enabled on the router. A sample message follows:

  ```
  VINES ping: VINES service is not running
  ```

Examples:

If you enter:	The system:

ping -vines 2705682.8003	Pings the device at the VINES address 2705682.8003 and waits up to 5 seconds (default) for a response. The console displays one of the following messages:
	`VINES ping: 2705682.8003 is alive`
	`VINES ping: 2705682.8003 does not respond`
	`VINES ping: 2705682.8003 is unreachable`

ping -vines 2705682.8003 -p	All of the above, but displays the intervening hop addresses to the destination before displaying the response message for each ping. For example, the console displays the following messages:
	`VINES ping: 809637039.1`
	`VINES ping: 809847041.1`
	`VINES ping: 2705682.8003 is alive (size = 16 bytes)`

ping -vines 2705682.8003 -t3 -r8	Pings the device at the VINES address 2705682.8003 eight successive times and waits up to 3 seconds for a response to each ping. The console displays one of the following for each ping sent:
	`VINES ping: 2705682.8003 is alive`
	`VINES ping: 2705682.8003 does not respond`
	`VINES ping: 2705682.8003 is unreachable`
	The console also displays the following type of message after reporting the progress of each ping:
	`VINES ping: 2705682.8003 responded to 8 out of 8: 100% success`

AppleTalk Ping

When you issue the **ping** command for AppleTalk to a remote AppleTalk device, it responds if it can be reached, and the console displays the response or the result of the request. AppleTalk **ping** uses the AppleTalk Echo Protocol.

Enter the following to ping a remote device running AppleTalk:

ping -at *<network_ID>.<node_ID>* [**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*]

<network_ID>.<node_ID> is the required AppleTalk address of the remote device, in the format of a 16-bit network number and an 8-bit node number.

Note: You can enter the network and node addresses in decimal or hexadecimal format. If you use hexadecimal format, precede each address with the 0x prefix.

[**-t***<timeout>*] [**-r***<repeat_count>*] [**-s***<size>*] are optional. These parameters are as follows:

<timeout> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 5.

<repeat_count> is the number of ping messages to send. The system does not wait for the timeout before sending the next ping. Enter a value between 0 and 10 (inclusive). The default is 1.

<size> is the number of bytes of data to send with each ping. The default is 16.

The console displays one of the following messages when you issue a **ping** command. (If you enter a value in the *<repeat_count>* argument, the system displays one of the following messages for the default ping, plus one for each additional ping):

- An `alive` message: This message appears if the system receives a response from the target device within the <*timeout*> allowed. The message also indicates the size of the test packet. A sample message follows:

  ```
  AT ping: 100.5 is alive (size = 16 bytes)
  ```

- A `does not respond` message: This message appears if the address of the target device is resolved, but the system does *not* receive a response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  AT ping: 100.5 does not respond
  ```

- A *<target_address>* `is unreachable` message: This message appears if the local Bay Networks router cannot find the specified address in its routing table. A sample message follows:

  ```
  AT ping: 100.5 is Unreachable
  ```

- A `resource error` message: This message appears if the local Bay Networks router cannot allocate a buffer for the request because none is available. A sample message follows:

  ```
  AT ping: resource error
  ```

- An `Invalid AppleTalk option` message: This message appears if you specify an invalid parameter (for example, **-p**). A sample message follows:

  ```
  AT ping: Invalid AppleTalk option
  ```

- An `Invalid AppleTalk address` message: This message appears if you specify an invalid address (for example, 1.2.3.4). A sample message follows:

  ```
  AT ping: Invalid AppleTalk address
  ```

- A `Specified size too large` message: This message appears if you specify a <*size*> that is larger than 585. The system uses the maximum of 585 bytes. A sample message follows:

  ```
  AT ping: Specified size too large; using maximum of 585 bytes
  ```

- An `AT service is not running` message: This message appears if the AppleTalk service is not enabled on the router. A sample message follows:

  ```
  AT ping: AT service is not running
  ```

Examples:

If you enter:	The system:

ping -at 100.5	Pings the device at the AppleTalk address 100.5 and waits up to 5 seconds (default) for a response. The console displays one of the following messages:
	`AT ping: 100.5 is alive`
	`AT ping: 100.5 does not respond`
	`AT ping: 100.5 is unreachable`

ping -at 100.5 -t3 -r8	Pings the device at the AppleTalk address 100.5 eight successive times and waits up to 3 seconds for a response to each ping. The console displays one of the following for each ping sent:
	`AT ping: 100.5 is alive`
	`AT ping: 100.5 does not respond`
	`AT ping: 100.5 is unreachable`
	The console also displays the following type of message after reporting the progress of each ping:
	`AT ping: 100.5 responded to 8 out of 8: 100% success`

APPN Ping

When you issue the **ping** command for APPN to a remote APPN device, it responds if it can be reached, and the console displays the response or the result of the request. APPN **ping** uses the APING (APPN Ping) Transaction Program (TP) to send an APING request to the APINGD TP running on the remote device.

Enter the following to ping a remote device running APPN:

ping -appn <*CP_name*> [**-t**<*timeout*>] [**-r**<*repeat_count*>] [**-s**<*size*>] [**-m**<*mode*>]

<*CP_name*> is the required APPN address, in the format of a Control Point name, of the remote device. Use the format <*network_ID*>.<*CP_name*> if the remote device is not on the same network as the system you are pinging from.

[**-t**<*timeout*>] [**-r**<*repeat_count*>] [**-s**<*size*>] [**-m**<*mode*>] are optional. These parameters are as follows:

<*timeout*> is the number of seconds for each ping to time out. If the system receives a response to a ping after it has timed out, the system does not send an "alive" message to the console. The default is 15.

<*repeat_count*> is the number of ping messages to send. The system does not wait for the timeout before sending the next ping. The default is 1.

<*size*> is the number of bytes of data to send with each ping. The default is 100.

<*mode*> is the mode name. Choices include #INTER, #BATCH, #INTERSC, and #BATCHSC. #INTER refers to the interactive mode (that is, where not much data is involved and response time is very important). #BATCH refers to a mode where a lot of data is involved, and response time is not important. #INTERSC and #BATCHSC are secure versions of #INTER and #BATCH. If you do not specify a mode, the mode defaults to a blank value.

The console displays one of the following messages when you issue a **ping** command:

- An `alive` message: This message appears if the system receives a response from the target device within the <*timeout*> allowed. A sample message follows:

  ```
  APPN ping: bay is alive
  ```

- A `did not complete in the time allowed` message: This message appears if the node is alive but congested, the data transfer time exceeded the timeout, or the directory search is not complete. A sample message follows:

  ```
  APPN ping: ping of bay did not complete in the time allowed
  ```

- An `unreachable` message: This message appears if no route could be calculated to the remote device or if the remote device does not support APINGD. A sample message follows:

  ```
  APPN ping: bay is unreachable
  ```

- An `invalid name` message: This message appears if the specified node name or mode name is invalid. A sample message follows:

  ```
  APPN ping: invalid name specified
  ```

- An `APPN service is not running` message: This message appears if the APPN service is disabled on the router. A sample message follows:

  ```
  APPN ping: APPN service is not running
  ```

Examples:

If you enter (on one line):	The system:

ping -appn raleigh	Pings the device at the APPN address raleigh and waits up to 15 seconds (default) for a response. The console displays one of the following messages:
	`APPN ping: raleigh is alive`
	`APPN ping: raleigh is unreachable`

ping -appn raleigh -r100 -s2000 -m#inter	Pings the device at the APPN address raleigh 100 successive times, sending 2000 bytes of data with each ping and specifying the interactive mode. The console displays one of the following messages:
	`APPN ping: ping of raleigh did not complete in the time allowed`
	`APPN ping: raleigh is alive`
	`APPN ping: raleigh is unreachable`

ping -appn raleigh -r10 -s2000 -m#batch -t100	Pings the device at the APPN address raleigh 10 successive times, sending 2000 bytes of data with each ping and specifying the batch mode and a timeout of 100 seconds The console displays one of the following messages:
	`APPN ping: ping of raleigh did not complete in the time allowed`
	`APPN ping: raleigh is alive`
	`APPN ping: raleigh is unreachable`

Displaying the ATM ARP Table for an Interface

You can display the ATM ARP tables for a specific IP interface address by entering the **atmarp** command during a Technician Interface session. The command has the following syntax and options:

atmarp table [*<options>*] *<IP_address>*

Option Flag	Purpose
-a	Displays ATM address for the *<IP_address>* you enter in the command line
-r	Displays the resolution table for the *<IP_address>* you enter in the command line
-v	Displays the Virtual Circuit (VC) table for the *<IP_address>* you enter in the command line
-l	Displays all (-r, -v, and -a) tables for the *<IP_address>* you enter in the command line

<IP_address> is the address of an IP interface on the ATM ARP client or server.

Examples (server):

```
[2:1]$ atmarp table -r 128.185.97.73

IP address     Life   ATM address                                  Vpi.vci
-------------  -----  -------------------------------------------  -------
128.185.97.74  423    39000000000000000000000000.0000a20d74aa01  0.63
```

```
[2:1]$ atmarp table -l 128.185.97.73

IP Address       State      Encaps     Lifetime  Retries
---------------  ---------  ---------  --------  --------
128.185.97.74    Resolved   Default    410       0
```

```
[2:1]$ atmarp table -v 128.185.97.73

Vpi.vci  Atm address                                  IP address     Life
-------  -------------------------------------------  -------------  ----
0.63     39000000000000000000000000.0000a20d74aa01  128.185.97.74  399
```

```
[2:1]$ atmarp table -a 128.185.97.73

ATM address                                Vpi.vci
-----------------------------------------  --------
39000000000000000000000000.0000a20d74aa01  0.63
```

Examples (client):

```
[2:1]$ atmarp table -v 128.185.97.74

Vpi.vci  Atm address                                IP address   Life
-------  -----------------------------------------  -----------  ----
0.63     39000000000000000000000000.00979797979700

[2:1]$ atmarp table -a 128.185.97.74

ATM address                                Vpi.vci
-----------------------------------------  --------
39000000000000000000000000.00979797979700  0.63
```

Chapter 4
Managing a NonVolatile File System

You can use the Technician Interface to manage nonvolatile file system (NVFS) files on a Bay Networks router.

When you manage an NVFS, you can

- Use multiple memory cards
- Name files
- Display the status of each memory card installed in the router
- Display a directory
- Change the active volume
- Copy a file from one volume to another, or to the same volume
- Transfer a file
- Display the contents of a file
- Delete a file
- Compact file space
- Format a memory card
- Partition a memory card or SIMM

Note: The NVFS automatically mounts and unmounts memory cards.

Overview

The NVFS file system on the router reads and writes to one or more memory cards. Memory cards exist in 2-MB, 4-MB, and 8-MB sizes. Each memory card provides system access to the software image and configuration file during a cold start. (A cold start occurs after a power-cycle or after you enter the **diags** command.)

Each FRE module (BLN, BLN-2, BCN) in a router can host one memory card. A Flash System Controller (VME-based routers only) in a router can host one or two memory cards. Multiple memory cards are optional in the router. The section that follows suggests how to manage multiple memory cards.

A volume number is the same number as the slot that hosts the memory card. For example, Volume 2 resides on Slot 2.

Table 4-1 outlines the NVFS commands. The Wildcard column indicates whether you can use wildcards (***** and **?**) when entering the commands. You use wildcards to display multiple filenames, and to copy or delete multiple files. The wildcards have the same meaning as those in UNIX:

- The ***** wildcard matches any number of characters, including zero characters.
- The **?** wildcard matches any single character. A match occurs only when a character is present in the position indicated by the wildcard.

The sections that follow describe the commands in detail. They also show how to use the wildcards.

Table 4-1. NVFS Commands

Command	Wildcard	Function
compact		Reallocates file space on a memory card.
cd		Changes the active volume.
copy	✔	Copies a file from one volume to another or to the same volume.
delete	✔	Deletes a file from a volume.
dinfo		Displays the volume number, status, and space for each volume.
dir	✔	Displays all files on a volume.
format		Erases any existing files on a volume and formats the volume.
partition		Partitions file system media into two volumes.
save		Saves the current software configuration, aliases, or events to a file. Refer to Chapter 6, 7, or 9 for instructions on the **save** command.
tftp		Transfers a file to or from the router.
type	✔	Displays the contents of a file in ASCII or hexadecimal format.

Using Multiple Memory Cards

This section describes how to manage multiple memory cards on the router. You may want to allocate them as follows:

- Keep one card as the primary card used for booting.
- Use another card for redundancy.

  If you are providing redundancy, be sure to copy files that you modify to the redundant volumes.
- Use another card as temporary storage for log files and test configuration files.

The system boots from the default router software image (Table 4-2) and configuration file (*config*) if you do not specify the boot image and configuration file when booting. Refer to Table 4-2 for a list of router software images associated with particular routers and processor modules.

Table 4-2. Router Software Images

Image	Router	Processor Module
ace.out	FN, LN, CN, ALN	ACE
afn.exe	AFN	Motorola
an.exe	AN, ANH	Motorola
asn.exe	ASN	Motorola
bn.exe	BLN, BLN-2, BCN	FRE-1, FRE-2

Caution: It is possible that the FRE modules can simultaneously load different images or configurations if you have alternate versions of the boot or configuration file. We recommend that you have only one version of each on the router. Assign new names to alternate versions.

Naming Files: Rules and Conventions

The rules for naming files are as follows:

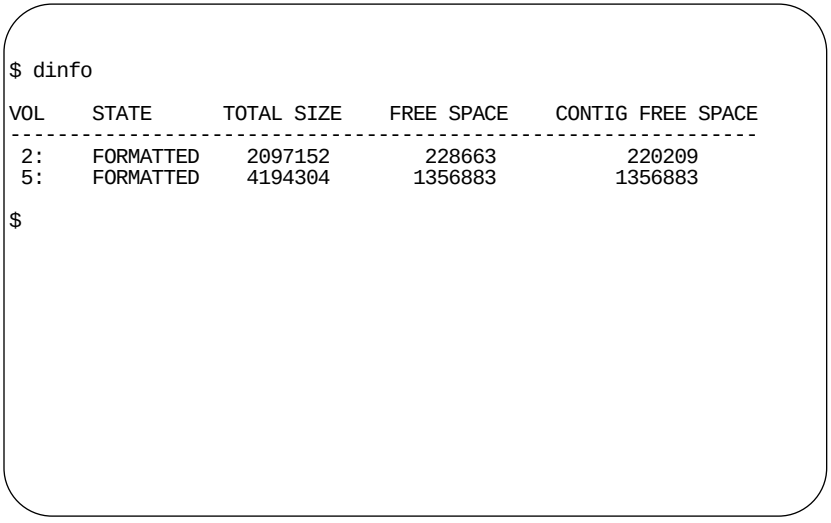
- You must specify the volume location (slot number) of any file you reference and of any file you create. The sections that follow detail the syntax requirements, including the slot number specification, for each command.
- Filenames must start with an alphabetical character. The remaining characters must be alphanumeric, and may also include the underscore (_) character and dot (.) character. Spaces are not allowed.
- Filenames can consist of one to 15 characters. We recommend a limit of 8 characters, however, to ensure that all operating systems that we support can recognize the names.
- File extensions are optional, and must be preceded by a filename and a dot. The total Technician Interface limit for the filename and file extension is 15 characters (including the dot).

We also recommend the following conventions when naming files so that you can easily distinguish files by type:

- Use the *.exe* file extension for router software images for the FRE® and Motorola modules (BLN, BLN-2, BCN, AFN, AN, ANH, and ASN). (The default router software images are *bn.exe*, *afn.exe*, *an.exe*, and *asn.exe*.)
- Use the *.out* file extension for router software images for the ACE modules (FN, LN, CN, and ALN). (The default router software image is *ace.out*.)
- Use the *.cfg* file extension for alternate configuration files. (The default configuration file is *config*.)
- Use the *.al* file extension for alias files.
- Use the *.log* file extension for log files.
- Use the *.bat* file extension for script files.

Displaying the Status of All Memory Cards

Enter **dinfo** to display the status of all memory cards currently installed in the router. Figure 4-1 shows a sample **dinfo** display of a system with memory cards installed in Slots 2 and 5.



```
$ dinfo

VOL    STATE       TOTAL SIZE    FREE SPACE    CONTIG FREE SPACE
-------------------------------------------------------------------
 2:    FORMATTED    2097152        228663          220209
 5:    FORMATTED    4194304       1356883         1356883

$
```

Figure 4-1. Sample Dinfo Display

The **dinfo** command displays the following data:

Vol: Slot number where the memory card is currently installed. (*Vol* is short for volume.)

State: Either *formatted* or *corrupted*. If you purchase a card from another supplier, the **dinfo** display may list it as *corrupted*. If a card is *corrupted*, format it. (Refer to "Formatting a Memory Card" later in this chapter for instructions.)

Total Size: Total number of bytes (used and unused) in the memory card.

Free Space: Number of unused bytes in the memory card.

Contig Free Space: Number of unused bytes in the largest block of available space in the memory card.

When you delete a file on a memory card, the file becomes inaccessible, but the data remains on the card. Eventually, all space is used. The **compact** command copies the active files to memory, erases the memory card, and copies the files back to the memory card. Refer to the section "Compacting File Space" to free up space to prevent or respond to a file allocation failure.

Displaying a Directory

Use the **dir** command to display a list of the files on a particular volume. You can enter the wildcard characters ***** and **?** to display filenames with the character strings you specify.

Enter the following to list the files stored on the active volume:

dir

Enter the following to list the files stored on a different volume, where <*vol*> is the slot number containing the volume:

dir <*vol*>**:**

The directory display shows an entry for each file on the volume. Each entry consists of a filename, size, and modification date/weekday/time. Figure 4-2 shows a sample response to the **dir** command on a BLN.

```
$ dir

 Volume in drive 5: is
 Directory of 5:

File Name             Size    Date     Day      Time
-------------------------------------------------------
pvc0.cfg              6872  10/14/94  Fri.    13:51:12
fr.al                 5616  09/16/94  Fri.    08:04:26
fr.VIII              10158  09/28/94  Wed.    15:25:48
mfg.log             172052  11/03/94  Thurs.  16:24:28
config                7132  11/11/94  Fri.    15:42:01
bn.exe             2635353  01/05/95  Thurs.  09:08:55

 4194304 bytes - Total size
 1356883 bytes - Available free space
 1356883 bytes - Contiguous free space

$
```

Figure 4-2. Sample NVFS Directory Listing

Examples:

If you enter:	The console:
dir	Displays the list of files on the active volume.
dir *.cfg	Displays the list of files with a *.cfg* extension on the active volume.
dir 3:	Displays the list of files on Volume 3.
dir 4:???.log	Displays the list of files with a three-character filename and a *.log* extension on Volume 4.

The factory-default filenames are as follows:

ace.out	The router software image for the FN, LN, CN, and ALN. You cannot read or change this file. The system automatically refers to this binary file for booting instructions unless you use the **boot** command to specify a different router software image.
afn.exe *an.exe* *asn.exe* *bn.exe*	The router software image for the AFN. The router software image for the AN and ANH. The router software image for the ASN. The router software image for the BLN, BLN-2, and BCN. You cannot read or change this file. The system automatically refers to this binary file for booting instructions unless you use the **boot** command to specify a different router software image.
afnboot.exe	A copy of the combined bootstrap PROM and diagnostics PROM image for an AFN router.
anboot.exe	A copy of the bootstrap image resident on the bootstrap PROM of an AN series router. You cannot read or change this file.
andiag.exe	A copy of the diagnostics image resident on the diagnostics PROM of an AN series router. You cannot read or change this file.
asnboot.exe	A copy of the bootstrap image resident on the bootstrap PROM of an ASN router. You cannot read or change this file.
asndiag.exe	A copy of the diagnostics image resident on an ASN router. You cannot read or change this file.
config	The default configuration file. The system refers to this binary file for configuration data when booting. You can change the configuration by copying an alternative configuration file to *config*. You can also use the **boot** command to specify a different configuration file. This file must have the *config* filename for the system to configure automatically after booting. We recommend that you copy *config* to a new backup filename before overwriting it.

debug.al	An ASCII file containing aliases (commands that abbreviate long or multiple commands) that you can use to debug common network problems. (Refer to "Debugging with Predefined Aliases" in Chapter 9 to use the aliases in this file.)
frediag.exe	A copy of the diagnostics image resident on the diagnostics PROM of a BLN, BLN-2, or BCN router. You cannot read or change this file.
freboot.exe	A copy of the bootstrap image resident on the bootstrap PROM of a BLN, BLN-2, or BCN router. You cannot read or change this file.
install.bat	A script file that you use during the initial startup.
ti.cfg	A configuration file containing the MIB variables associated with the default Technician Interface console operating parameters. This file contains the minimal configuration necessary to operate the router. This file is stored in binary format.

The Total size, Available free space, and Contiguous free space fields that appear below the **dir** display show the same information as the Total Size, Free Space, and Contig Free Space in the **dinfo** display. Refer to the earlier section "Displaying the Status of All Memory Cards" for a description of these fields.

Changing the Active Volume

Use the **cd** command to change the active volume, as follows:

cd *<vol>***:**

<vol> is the slot number of the volume:

The system displays the new active volume.

If you enter the cd command without specifying a volume, the system displays the present working directory, as follows:

cd

```
Present Working Directory: 2:
```

Copying a File

Use the **copy** command to make a copy of a file. You can use the wildcard characters ***** and **?** when issuing the **copy** command to copy multiple files.

Caution: The system automatically overwrites any file already on the volume that has the same filename as the file you are creating. To avoid overwriting an existing file, display a directory of the volume's contents and determine the filenames that are already in use.

Enter the following to copy a file on the active volume:

copy *<old_file> <new_file>*

Enter the following to copy a file to a different volume:

copy *<vol>*:*<old_file> <vol>*:*<new_file>*

<vol> in *<vol>:<old_file>* is the slot number of the source volume.

<vol> in *<vol>:<new_file>* is the slot number of the target volume.

Copying Files from NVFS to DOS

When copying files from NVFS to DOS on FN, LN, or CN routers equipped with Flash System Controllers, make sure that the NVFS filename contains no more than eight characters with an optional extension of no more than three characters preceded by a dot (*xxxxxxxx.xxx*). NVFS filenames can consist of one to 15 characters; DOS filenames can consist of one to eight characters with an optional one- to three-character extension. When the DOS operating system receives a filename that contains more than eight characters, it truncates the filename.

Examples:

If you enter:	The system copies:
copy config alt.cfg	The *config* file on the active volume and names the copy *alt.cfg*.
copy 3:alt.cfg	The *alt.cfg* file on Volume 3 and stores the copy, also named *alt.cfg*, on the active volume.
copy 2:l6_22.log 2:sp.log	The *l6_22.log* file on Volume 2 and names the copy *sp.log*.
copy 2:config 3:config	The *config* file on Volume 2 and stores the copy, also named *config*, on Volume 3.
copy *.* 3:	All files from the active volume to Volume 3.
copy 2:*.exe 4:	All executable files from Volume 2 to Volume 4.
copy 3:???.* 4:	All files with a filename of three characters from Volume 3 to Volume 4.

Note: You cannot copy from NVFS to DOS on an AFN, which allows only one file system (NVFS) to be available after a system boot.

Transferring a File

Depending on conditions existing within your network, you can transfer files between Bay Networks routers and remote workstations using either of two methods:

- In-band (using Technician Interface **tftp** commands and a route through your high-speed, IP network)
- Out-of-band (using Technician Interface **xmodem** commands and a route through a lower-speed, dial network)

You can transfer a file in-band whenever

- You can dial in to the Technician Interface port of a router you choose as source or destination for a file transfer operation
- An operational IP routing path exists through your network, between the file source (a router or a remote workstation) and the file destination (also a router or a remote workstation)

Out-of-band file transfers are typically a less efficient but sometimes useful method, for example, for router diagnosis and management.

You use this method most beneficially when

- You can dial in to the Technician Interface port of a router you choose as the source or destination for a file transfer operation
- All IP routing paths between the file source and the file destination are down (nonoperational)

You can use either a UNIX or a 386/486 DOS remote workstation to transfer files in-band or out-of-band using Technician Interface **xmodem** commands, as operating conditions within your network allow.

In-Band File Transfers

The **tftp** command invokes the Trivial File Transfer Protocol (TFTP) software to transfer a file between a Bay Networks router and another router or host capable of serving **tftp** file transfer requests.

The TFTP software resides within the IP router. Consequently, you must load TFTP on the router and enable it (refer to *Quick-Starting Routers and BNX Platforms* for instructions).

When you transfer a file to a Bay Networks router, unless you specify the target volume, the TFTP server of the receiving (client) router uses the value of the wfTftp.2.0 MIB attribute to determine the target volume.

For example, if you enter

tftp put 192.*xx.x.xx* 2:config

where **192.*xx.x.xx*** is a valid IP address, the file *config* will be called *config* on the router at the specified IP address and will go to the volume specified in wfTftp.2.0. The same will happen if you enter

tftp put 192.*xx.x.xx* 2:config new_config

except that the file will be called *new_config*.

However, if you enter

tftp put 192.*xx.x.xx* 2:config 3:test_config

the file *config* will now be called *test_config* and reside on Volume 3, overriding whatever is in wfTftp.2.0.

The wfTftp.2.0 attribute is set during the Quick-Start procedure, using the *debug.al* alias **setvol** <*slot no.*> to target an NVFS volume or **setvol 65** to target a DOS volume.

Caution: The destination system in a file transfer automatically overwrites any file already on its volume that has the same filename. If enough space does not exist on the file system for the new file, and the new file has the same name as an old file, the old file will be destroyed and the new file will be corrupted. This is because TFTP copies the new file over the old and runs out of space before completing the copy. Be sure to follow the instructions in this section to avoid corrupting the config file.

If the destination system has a memory card to which you are transferring a file, we recommend that you compact it first to optimize the space available for the file. Refer to "Compacting File Space," later in this chapter, for instructions.

We recommend that you first copy the file at the source to a new, temporary filename if the name is the same as an existing filename at the destination.

Enter the following commands to initiate a file transfer from the Technician Interface:

tftp get *<host_address> <remote_vol>:<remote_file>* [*<local_vol>*]:[*<local_file>*]

tftp put *<host_address> <remote_vol>:<remote_file>* [*<local_vol>*]:[*<local_file>*]

get means you are transferring the file to the local Bay Networks router and **put** means you are transferring the file to the remote node.

<host_address> is the address of the host for transfers.

<remote_vol> is the volume number containing the volume to which you want to transfer the file.

<remote_file> is the name to which you want to transfer the file. If you do not enter a destination name, the system defaults to the *<local file>* you specified for the source file.

<local_vol> is the volume number containing the volume in the local Bay Networks router.

<local_file> is the name of the file used on the local router.

Caution: The local system erases the file if you enter its address in the *<host_address>* field of the **tftp** command.

The system executes one TFTP request at a time for the duration of the file transfer. The destination system stores the file under the name you specify. If you do not enter a destination name, the system defaults to the source filename.

Examples:

If you enter (on one line):	The local system:
tftp put 192.32.1.62 2:config2.cfg 3:newconf	Sends a copy of *config2.cfg* from Volume 2 to *newconf* in Volume 3 on the remote node at the IP address 192.32.1.62.
tftp get 192.32.1.62 2:config2.cfg	Requests a copy of *config2.cfg* from Volume 2 of the remote node at the IP address 192.32.1.62 and stores the copy in the current working directory.
tftp put 192.32.1.62 2:config2.cfg	Sends a copy of *config2.cfg* to *config2.cfg* in Volume wfTftp.2.0 on the remote node at the IP address 192.32.1.62.
tftp put 192.32.1.62 2:config2.cfg 3:config3.cfg	Sends a copy of *2:config2.cfg* but puts it on Volume 3 and calls it *config3.cfg*.

After transferring the file, you can copy it at the source to its original name. If the new file at the destination is a configuration file or an executable file, verify its integrity by booting with it. If the system boots and loads the configuration without problems, you can rename or copy the filename at the destination to its original.

You can also load a file onto the router by specifying the router host name and volume, using the following command:

tftp put *<remote_file> <host_name>*:*<local_vol>*:*<local_file>*

This method is useful if the wfTftp.2.0 attribute for the default volume was not set during the Quick-Start procedure.

Example:

If you enter:	The local system:
tftp dark **put install.bat dark:2:install.bat**	Transfers a copy of the *install.bat* file to Volume 2 on the router known as "dark."

Out-of-Band File Transfers

Appendix B in this guide describes how to transfer files out-of-band (via the dial telephone network), by means of the **xmodem** command.

Displaying the Contents of a File

Use the **type** command to display the contents of a file. Before displaying a file, enter **more on** to display the file one screen at a time.

Enter the following to display a file:

type [**-x**] *<vol>*:*<filename>*

-x is an optional argument to display the file in hexadecimal format. This allows files containing nonprintable information to be viewed.

<*vol*> specifies the slot number of the volume containing the file.

<*filename*> is the name of the file you are displaying.

The file is displayed in the same format in which it is stored (provided that you do not enter the **-x** argument): binary for log files and ASCII for alias files. Log files are stored in binary format; use the **log** command described in "Logging and Displaying Event Messages" in Chapter 6 to display a log file in ASCII format.

Examples:

If you enter:	The console:
type 2:install.bat	Displays the contents of the *install.bat* file, which is stored on the volume in Slot 2.
type -x 3:config	Displays the *config* file, which is stored on the volume in Slot 3. This file is displayed in hexadecimal format.

Deleting a File

Use the **delete** command to delete files that you specify. You can use the wildcard characters ***** and **?** when issuing the **delete** command.

Caution: You cannot recover a file after it is deleted. The **delete** command does not prompt you to verify a deletion.

Enter the following to delete a file on the active volume:

delete *<filename>*

Enter the following to delete a file on a different volume:

delete *<vol>*:*<filename>*

<*vol*> is the slot number of the volume containing the file.

<*filename*> is the name of the file.

You can enter **del** or **delete** when deleting a file.

Examples:

If you enter:	The system:
delete alt.cfg	Deletes the *alt.cfg* file on the active volume.
delete 2:l6_22.log	Deletes the *l6_22.log* file on Volume 2.
delete 3:*.log	Deletes all files with the *log* filename extension on Volume 3.
delete 4:???.log	Deletes all files with a three-character filename and a *log* filename extension on Volume 4.

Compacting File Space

When you delete a file from a memory card, the file and its data become inaccessible and eventually occupy all remaining storage space on that card. Use the **compact** command to

- Copy active files to memory
- Erase the card's contents
- Copy the active files back to the memory card

If responses to the **dir** or **dinfo** commands reveal more free space than contiguous free space on a memory card, compacting the space on the card increases the contiguous free space.

Caution: Back up the files by copying them to a second memory card before issuing the **compact** command.

Enter the following to erase the memory card contents and rewrite its files, where <*vol*> is the slot number of the card:

compact <*vol*>**:**

The following message appears:

```
Compacting file system on volume <vol>:...
This may take several minutes...Please wait...

100% Complete

Compaction completed
```

The space is compacted when the Technician Interface prompt reappears.

Formatting a Memory Card

Use the **format** command to erase all files on a memory card and format it, where <*vol*> is the slot number of the card:

format <*vol*>**:**

Use the **format** command to format new memory cards if you do not obtain them from Bay Networks.

Enter **dinfo** to ensure that the file system formatted the card successfully.

Caution: You cannot recover your files after entering the **format** command. We recommend that you copy them to a second volume before issuing the **format** command.

Transferring a File to a Full Memory Card

If you attempt to transfer a file to a memory card that does not have enough space, the name of the file with a length of 0 bytes appears in the memory card's directory. Before you transfer another file to the memory card, you should optimize the available space by completing the following steps:

1. **Delete the file from the memory card, using the delete command.**
2. **Compact the file system, using the compact command.**

Partitioning a Memory Card or SIMM

Memory partitioning enables you to use commands such as the **compact** command on one partitioned volume at a time. Partitioning also enables you to store copies of boot images and configuration files on each partition to provide redundancy.

The **partition** command only works with a 4-MB or greater memory card or SIMM used with an AN or ASN loaded with Version 8.10 or later router software. The command creates or deletes a partition on a specified volume, or on the present working volume if a volume is not specified. Such partitioning provides two independent file systems on two independent volumes.

Enter the following commands to partition the memory card or SIMM or delete a memory partition:

partition create [<*vol*>:]

partition delete [<*vol*>:]

When creating a partition, the current file system cannot exceed one-half the total media size. For example, if you are using a 4-MB memory card that contains files totaling more than 2 MB, you need to remove or edit some of those files until they total 2 MB or less.

Once the partition has been created, the new volume is referred to as <*vol*>b, and the existing volume is referred to as either <*vol*>a or <*vol*>.

Caution: Be careful when deleting a partition. When you issue the **partition delete** command without specifying a subvolume, all files on <*vol*>b are lost.

Examples:

If you enter:	The system:
partition create 1:	Divides memory card or SIMM Volume 1 into two volumes, storing all existing files in Volume 1a and creating and formatting a new Volume 1b.
partition delete 1b: or **partition delete 1:**	Removes Volume 1b (files included).

Chapter 5
Managing a DOS File System

You can use the Technician Interface to manage DOS files on a Bay Networks router. This chapter is intended only for users whose routers are equipped with a diskette drive.

To manage a DOS file system, you do the following:

- Name files
- Mount and unmount a volume
- Change the present working directory
- Display a directory
- Label a diskette
- Create and remove a directory
- Rename a file or directory
- Copy files to different filenames on the same directory, or to a different directory
- Transfer a file
- Change a file's attributes
- Display the contents of a file
- Delete a file

Overview

The DOS file system on the router reads and writes to the diskette. The diskette gives the system access to the software image and configuration file during a cold start. (A cold start occurs after a power-cycle.)

The DOS file system accepts the DOS commands that you use to manage the files and directories on the diskette. (For a list of these commands, refer to Table 5-1.)

To alert the system that the diskette is available for access, issue the **mount a:** command. DOS performs an implied mount if you issue any of the DOS file management commands listed in Table 5-1 (except, of course, the **unmount** command).

Caution: Be sure to issue the **unmount** command as described in this chapter before you remove a diskette, reboot the router, or reset Slot 2. File corruption errors can occur when you perform these tasks without first issuing the **unmount** command.

The Wildcard column indicates whether you can use wildcards (***** and **?**) when entering the commands. You use wildcards to display multiple filenames, and to copy or delete multiple files. The wildcards have the same meaning as those in UNIX:

- The ***** wildcard matches any number of characters, including zero characters.
- The **?** wildcard matches any single character. A match occurs only when a character is present in the position indicated by the wildcard.

Note: The DOS file system in the router does not format diskettes; however, you can format them on a PC and use them in the router.

Table 5-1. DOS File Management Commands

Command	Wildcard	Function
attr	✔	Changes file attributes.
copy	✔	Copies a file from one directory to another or to the same directory.
cd		Changes the present working directory.
delete	✔	Deletes a file.
dir	✔	Displays all files in a directory.
label		Changes the internal label of the diskette.
mkdir		Creates a directory.
mount		Makes the diskette drive available.
rename	✔	Renames file and directories.
rmdir		Removes a directory.
save		Saves the current software configuration, aliases, or events to a file. Refer to Chapter 6, 7, or 9 for instructions on the **save** command.
tftp		Transfers a file to or from the router.
type	✔	Displays the contents of a file in ASCII or hexadecimal format.
unmount		Makes the diskette drive unavailable.

The sections that follow describe the commands in detail. They also show how to use the wildcards.

Naming Files and Directories

The rules for naming files and directories are as follows:

- Filenames and directory names must start with an alphabetical character. The remaining characters must be alphanumeric, and may also include the underscore (_) character. Spaces are not allowed.
- DOS directory names and filenames can consist of one to eight characters.

- You can specify a directory or filename in upper- or lowercase letters; however, in directory listings and other displays, DOS shows all directory and filenames in upper case.
- File extensions are optional, and must be preceded by a dot. They can be from one to three characters.

Also, we recommend that you use the following conventions when naming files so that you can distinguish files by type.

- Use the *.exe* file extension for software images for the FRE and other modules (BLN, BLN-2, BCN, AFN, AN, ANH, and ASN). (The default software images are *bn.exe*, *afn.exe*, *an.exe*, and *asn.exe*.)
- Use the *.out* file extension for software images for the ACE modules (FN, LN, CN, and ALN). (The default software image is *ace.out*.)
- Use the *.cfg* file extension for alternate configuration files. (The default configuration file is *config*.)
- Use the *.al* file extension for alias files.
- Use the *.log* file extension for log files.
- Use the *.bat* file extension for script files.

Mounting a Volume

Use the **mount** command to make the diskette drive available. Issue the following command when you install a diskette:

mount a:

The screen displays a File System Check Report (Figure 5-1).

```
$ mount a:
Device label:
Directory: A:\

File System Check Report:
     Allocated but unused clusters      : 0
     Used but unallocated clusters      : 0
     Cluster chains shared between files: 0
     File size is wrong                 : 0
     Missing EOF                        : 0
     Directory errors                   : 0
```

Figure 5-1. Mounting a Volume

The File System Check Report indicates the number of errors on a diskette. All values should be zero. Nonzero values indicate file corruption. Refer to the description of these values and to the DOS events in the log to determine the cause. The most common cause of file corruption is that DOS was interrupted while writing to the diskette and was unable to complete its operation. This can occur when the power resets, the router reboots, or Slot 2 is reset. You can avoid corrupting files when performing these tasks by first entering the **unmount** command (described next), and making sure the system does not respond with an error message indicating that a file is in use.

The File System Check Report entries are as follows:

- `Allocated but unused clusters` shows the number of reserved sectors not allocated to files.

  The router may in some cases be able to recover from this error when mounting the volume. The Technician Interface displays a message indicating success or failure after a recovery attempt. Enter the **unmount a:** and **mount a:** commands to determine whether DOS fixes the error. If the file system comes up clean, the error is fixed. If an error is detected again, use the check disk (**chkdsk**) command with the fix (/F) switch on a PC to free the allocated but unused sectors.

- `Used but unallocated clusters` shows the number of unreserved sectors allocated to files. The directory is corrupt.

  Use a PC to reformat the diskette.

- `Cluster chains shared between files` shows the number of sector chains that are allocated to more than one file.

  Use the **chkdsk** command on a PC to determine which files are corrupt, and delete those files.

- `File size is wrong` shows the number of File Allocation Table (FAT) entries and directory table entries that do not match.

  Use a PC to reformat the diskette.

- `Missing EOF` shows the number of files in the FAT that are missing an End of File (EOF) marker.

  Use a PC to reformat the diskette.

- `Directory errors` shows the number of errors in the directory.

  Refer to the log. Use a PC to reformat the diskette if necessary.

Unmounting a Volume

Use the **unmount** command to make the diskette drive unavailable before you remove a diskette, reboot the router, or reset Slot 2. When you issue the **unmount** command without using a **-f** argument, the system reports an error if files are in use at the moment you issue the command.

To unmount the currently active volume, make sure the diskette drive LED is off, and enter the command as follows:

unmount

The system reports an error if a file is in use at the moment you issued the command. Otherwise, you can assume that the unmount was executed. If the system reports an error, make sure the diskette drive LED is off and retry until no error is reported.

You can use the **-f** argument to force an unmount, regardless of whether a file is in use.

Caution: Use the **-f** argument to force an unmount only in emergencies. File corruption errors may occur when you force an unmount while DOS is writing to the diskette.

Enter the command as follows to force an unmount:

unmount -f

Changing the Working Directory

Use the **cd** command to change the present working directory. You can also use this command to display the present working directory. Enter the following command to display the present working directory:

cd

Enter the following command to change to another working directory:

cd *<dir_name>*

Examples:

If you enter:	The system:
cd	Displays the present working directory.
cd \old	Changes the present working directory to the subdirectory *old*.
cd \old\logs	Changes the present working directory to the subdirectory *old\logs*.
cd ..	Changes the present working directory to the parent directory.
**cd **	Changes the present working directory to the root directory.

Displaying a Directory

Use the **dir** command to display a list of the files in a directory. You can enter the wildcard characters ***** and **?** to display filenames with the character strings you specify. You cannot use wildcard characters in the directory portion of the pathname.

Enter the following command to list the files stored in the default directory:

dir

Enter the following command to display selected contents of another directory, where <*dir_name*> is the path to the directory and <*filename.ext*> is the file specification you want to display:

dir **<*pathname*>**<*filename.ext*>

Figure 5-2 shows a sample response to the **dir** command. The screen shows an entry for each file on the volume. Each entry consists of a filename, size, modification date/weekday/time, and attributes.

```
$ dir a:
Performing mount check...

 Volume in drive A: is
 Directory of A:\

File Name             Size    Date     Day      Time    Attributes
-------------------------------------------------------------------
.                        0  01/01/92  Wed.    12:00:00  -d----
..                       0  01/01/92  Wed.    12:00:00  -d----
ACE.OUT            1302081  01/04/95  Wed.    02:30:22  a-----
TI.CFG                 184  09/13/94  Tues.   23:40:58  a-----
CONFIG                 184  06/15/94  Wed.    22:35:04  a-----
TOMACIP               1760  06/16/94  Thurs.  00:54:18  a-----
TOMAC.CFG             3544  08/16/94  Tues.   23:07:00  a-----
AURP.CFG              4264  10/04/94  Tues.   04:44:48  a-----

 1474560 bytes - Total size
  143872 bytes - Available free space
```

Figure 5-2. Sample DOS Directory Listing

Examples:

If you enter:	The system:
dir	Displays the list of files in the present working directory.
dir *.cfg	Displays the list of files with a *.cfg* extension in the present working directory.
dir ???.log	Displays the list of files with a three-character filename and a *.log* extension in the present working directory.

The factory-default filenames are as follows:

ace.out	The router software image for the FN, LN, CN, and ALN. You cannot read or change this file. The system automatically refers to this binary file for booting instructions unless you use the **boot** command to specify a different router software image.
afn.exe	The router software image for the AFN.
bn.exe	The router software image for the BLN, BLN-2, and BCN. You cannot read or change this file. The system automatically refers to this binary file for booting instructions unless you use the **boot** command to specify a different router software image.
afnboot.exe	A copy of the combined bootstrap PROM and diagnostics PROM image for an AFN router.
config	The default configuration file. The system refers to this binary file for configuration data when booting. You can change the configuration by copying an alternative configuration file to *config*. You can also use the **boot** command to specify a different configuration file. This file must have the *config* filename for the system to configure automatically after booting. We recommend copying *config* to a new backup filename before overwriting it.
debug.al	An ASCII file containing aliases (commands that abbreviate long or multiple commands) that you can use to debug common network problems. (Refer to "Debugging with Predefined Aliases" in Chapter 9 to use the aliases in this file.)
frediag.exe	A copy of the diagnostics image resident on the diagnostics PROM of a BLN, BLN-2, or BCN router. You cannot read or change this file.
freboot.exe	A copy of the bootstrap image resident on the bootstrap PROM of a BLN, BLN-2, or BCN router. You cannot read or change this file.

install.bat	A script file that you use during the initial startup.
ti.cfg	A configuration file containing the MIB variables associated with the default Technician Interface console operating parameters. This file contains the minimal configuration necessary to operate the router. This file is stored in binary format.

Table 5-2 identifies the DOS file attributes that can appear in a DOS directory display, and their meanings. Refer to "Changing File Attributes" later in this chapter for more information about file attributes.

Table 5-2. DOS File Attributes

Attribute Flag	Meaning
a	Archive needed
d	Subdirectory
v	Volume ID
s	System file
h	Hidden
r	Read-only file

Labeling a Diskette

Use the **label** command to change or display a diskette's internal label. Enter the following to display the internal label:

label

Enter the following to change the internal label, where <*diskette_name*> is the new label:

label <*diskette_name*>

The name you enter may be from one to 11 characters. You can use letters, numbers, symbols, or spaces. But you cannot enter the following characters:

' " / \ { } : * | < > + = ; : ? ( ) & ^

Examples:

If you enter:	The system:
label	Displays the internal label of the diskette.
label disk1	Writes the internal label disk1 to the diskette.

Creating a Directory

Use the **mkdir** command to create a new directory. Enter the following to create a new directory, where <*dir_name*> is the new directory name you are creating, and <*pathname*> is the name of the path to that directory:

mkdir **<*pathname*>**<*dir_name*>

Examples:

If you enter:	The system:
mkdir logs	Creates a new subdirectory called *logs*.
mkdir \logs\L_6_23	Creates a new subdirectory called *L_6_23* in the path called *logs*.

Removing a Directory

Use the **rmdir** command to remove an existing directory. The directory must be empty before it can be removed. Enter the following to remove a directory, where <*dir_name*> is the directory name you are removing, and <*pathname*> is the name of the path to that directory:

rmdir **<*pathname*>**<*dir_name*>

Examples:

If you enter:	The system:
rmdir \logs\L_6_23	Deletes the subdirectory called *L_6_23* in the logs path.
rmdir logs	Deletes the subdirectory called *logs*.

Renaming a File or Directory

Use the **rename** command to change a filename or directory name.

If you specify a path to the file or directory, the file is moved to the new directory. The new file or directory must reside on the same diskette as the original. You can use the wildcard characters ***** and **?** to rename files and directories with the character strings you specify. Enter the following to rename a file or directory:

rename *<old_name> <new_name>*

Note: You cannot rename a file whose attributes are **h** (for hidden) or **s** (for system). Refer to the "Changing File Attributes" section, later in this chapter, for instructions on changing these protections.

Examples:

If you enter:	The system:
rename new.cfg old.cfg	Changes the file named *new.cfg* in the present working directory to *old.cfg*.
rename *.cfg *.arc	Changes all filenames with a *.cfg* extension to have a *.arc* extension in the present working directory.
rename \logs\l6_22.log \inv\span.log	Moves the *l6_22.log* file in the *logs* directory to the *inv* directory and renames the file to *span.log*.

Copying a File

Use the **copy** command to make a copy of a file. You can use the wildcard characters ***** and **?** when issuing the **copy** command to copy multiple files. The new file must reside on the same diskette as the original. (Use a PC to copy a file from one diskette to another.)

Caution: The system automatically overwrites any file in the directory that has the same filename as the file you are copying. To avoid overwriting an existing file, display the directory and determine the filenames that are already in use.

Enter the following command to copy a single file in the present working directory and rename the new version of the file:

copy *<old_name.ext> <new_name.ext>*

Enter the following command to copy a file from one directory to another, and use the same filename:

copy *<*dir_1*>*****<*old_name.ext*> *****<*dir_2*>

Enter the following command to copy a file from one directory to another, and use a new filename:

copy *<*dir_1*>*****<*old_name.ext*> *****<*dir_2*>*****<*new_name.ext*>

Examples:

If you enter:	The system:
copy config alt.cfg	Copies the *config* file in the present working directory and names the new copy *alt.cfg*.
copy *.* \newfiles	Copies all files in the present working directory to the directory *newfiles*.
copy \logf\l6_22.log \inv\span.log	Copies the *l6_22.log* file from the *logf* directory to the *inv* directory and names the new file *span.log*.

Copying Files from DOS to NVFS

When copying files from DOS diskettes to NVFS memory cards, you must specify the destination filename in the command. DOS filenames are in upper case. The NVFS filenames for the router software image and the configuration file must be in lower case.

Caution: The router will fail to boot from a memory card whose image and configuration file have uppercase names.

If you copy files from DOS diskettes to NVFS memory cards and you do not specify the destination filename, the system copies the filename in upper case. For example, if you enter **copy a:ace.out 1:,** the system copies the file to NVFS as *ACE.OUT*. If you enter **copy a:ace.out 1:ace.out**, the system copies the file to NVFS as *ace.out*.

Do not use wildcards. If you copy files from DOS to NVFS using a wildcard, the filenames will be copied in upper case. For example, if you enter

copy a:b*.exe 2:

the system copies all files that begin with the letter b and end with the file extension *.exe* to NVFS in the format B*XXXXXXX*.EXE, where *XXXXXXX* represents the missing characters in the filename.

Transferring a File

Depending on conditions existing within your network, you can use either of two methods of performing file transfers to and from Bay Networks routers and remote workstations.

The methods are

- In-band (using Technician Interface **tftp** commands and a route through your high-speed IP network)
- Out-of-band (using Technician Interface **xmodem** commands and a route through a lower-speed, dial network)

You can transfer a file in-band whenever

- You can dial in to the Technician Interface port of a router you choose as the source or destination for a file transfer operation
- An operational IP routing path exists through your network, between the file source (a router or a remote workstation) and the file destination (also a router or a remote workstation)

Out-of-band file transfers are typically a less efficient but sometimes useful method, for example, for router diagnosis and management.

You use this method most beneficially when

- You can dial in to the Technician Interface port of a router you choose as the source or destination for a file transfer operation
- All IP routing paths between the file source and the file destination are down (nonoperational)

You can use either a UNIX or a 386/486 DOS remote workstation to transfer files in-band or out-of-band using Technician Interface **xmodem** commands, as operating conditions within your network allow.

In-Band File Transfers

The **tftp** command invokes the TFTP software to transfer a file between a Bay Networks router and another router or host capable of serving **tftp** file transfer requests.

The TFTP software resides within the IP router. Consequently, you must load the TFTP software on the router and enable it (refer to *Quick-Starting Routers and BNX Platforms* for instructions). Also, when you transfer a file to a Bay Networks router, the TFTP driver of the receiving (client) router uses the value of the wfTftp.2.0 MIB attribute to determine the target volume. This attribute is set during the Quick-Start procedure, using the *debug.al* alias **setvol 65** to target the DOS volume.

Caution: The destination system in a file transfer automatically overwrites any file already on its volume that has the same filename. If enough space does not exist on the file system for the new file, and the new file has the same name as an old file, the old file will be destroyed and the new file will be corrupted. This is because TFTP copies the new file over the old and runs out of space before completing the copy. Be sure to follow the instructions in this section to avoid corrupting the config file.

We recommend that you first rename or copy the file at the source to a new, temporary filename if the name is the same as an existing file at the destination.

Enter the following command to initiate a file transfer from the Technician Interface:

tftp [**get** | **put**] *<remote IP address>* *<filename>* [*<filename>*]

[**get** | **put**] is **put** if you are transferring the file to the remote node and **get** if you are transferring the file to the local router.

<*remote_IP_address*> is the address of the remote node.

<*filename*> is the name of the file to be transferred.

[<*filename*>] is the name to which you want to transfer the file. If you do not enter a name, the system defaults to the <*filename*> you specified for the source file.

Caution: The local system erases the file if you enter its address in the *<remote_IP_address>* field of the **tftp** command.

The system executes one TFTP request at a time for the duration of the file transfer. The destination system stores the file under the name you specify. If you do not enter a destination filename, the system defaults to the source filename.

Examples:

If you enter:	The local system:
tftp put 192.32.1.62 config2.cfg newconf	Sends a copy of *config2.cfg* to *newconf* on the remote node at the IP address 192.32.1.62.
tftp get 192.32.1.62 config2.cfg	Gets a copy of *config2.cfg* from the remote node at the IP address 192.32.1.62.

After transferring the file, you can rename or copy it at the source to its original name. If the new file at the destination is a configuration file or an executable file, verify its integrity by booting with it. If the system boots and loads the configuration without problems, you can rename or copy the filename at the destination to its original name.

You can also load a file onto the router by specifying the router host name and volume, using the following command:

tftp put *<remote_file> <host_name>:<local_vol>:<local_file>*

This method is useful if the wfTftp.2.0 attribute for the default volume was not set during the Quick-Start procedure.

Example:

If you enter:	The local system:
tftp dark **put install.bat dark:2:install.bat**	Transfers a copy of the *install.bat* file to Volume 2 on the router known as “dark.”

Out-of-Band File Transfers

Appendix B in this guide describes how to transfer files out-of-band (using facilities outside the IP network), using the **xmodem** command.

Changing File Attributes

The **attr** command changes the DOS file attributes. These attributes are displayed when you enter the **dir** command. You cannot delete or rename a file whose attributes are **s** (for system) or **h** (for hidden). This section describes how to reassign attributes to such files, so that you can remove these protections.

Hexadecimal values with a 0x prefix determine the set of attributes associated with DOS files. Determine which hex value is associated with the set of attributes you want for a file. Then enter the **attr** command, along with the hex value and the name of the file(s) whose attributes you are assigning.

Enter the following to assign one or more attributes to a file in the present working directory:

attr *<hex_value> <filename.ext>*

Enter the following to assign one or more attributes to a file in another directory:

attr *<hex_value>* *****<*pathname*>*****<*filename.ext*>

You can use the wildcard characters ***** and **?** when naming files. Table 5-3 lists the DOS file attributes, their meanings, and their hex values.

Table 5-3. DOS File Attribute Hex Values

Attribute Flag	Meaning	Hex Value
a	Archive needed	0x20
d	Subdirectory	0x10 -- not user modifiable
v	Volume ID	0x08 -- not user modifiable
s	System file	0x04
h	Hidden	0x02
r	Read-only file	0x01

To assign a single attribute to a file, use the hex value associated with the attribute you want in the attribute command. For example, enter the following command to assign the read-only file attribute to a file named *config* located in the present working directory:

attr 0x01 config

To assign multiple attributes to a file, add the hex values associated with the attributes you want and enter the total in the attribute command. For example, to assign the attributes archive needed, hidden, and read-only to the *config* file, add their associated hex values:

0x20 + 0x02 + 0x01 = 0x23

Then enter the following command to assign these file attributes:

attr 0x23 config

You can also assign attributes to a file in another directory by specifying the pathname. For example, enter the following command to change the file attributes of a file named *l6_23.log* in the *logs* path:

attr 0x23 \logs\l6_23.log

Examples:

If you enter:	The system:
attr 0X01 config	Sets the attribute of the file *config* to read-only.
attr 0X03 config	Sets the attributes of the file *config* to hidden and read-only.
attr 0X23 config	Sets the attribute of the file *config* to hidden, read-only, and archive needed.

Displaying the Contents of a File

Use the **type** command to display the contents of a file. Before displaying a file, enter **more on** to display the file one screen at a time.

Enter the following to display a file:

type [**-x**] *<filename>*

-x is an optional command to display the file in hexadecimal format. This allows files containing nonprintable information to be viewed.

<*filename*> is the name of the file you are displaying.

The file is displayed in the same format in which it is stored (provided that you do not enter the **-x** argument): binary for log files and ASCII for alias files. Log files are stored in binary format; use the **log** command described in "Logging and Displaying Event Messages" in Chapter 6 to display a log file in ASCII format.

Examples:

If you enter:	The console displays:
type install.bat	The contents of the *install.bat* file.
type -x config	The *config* file in hexadecimal format.

Deleting a File

Use the **delete** command to delete files that you specify. You can use the wildcard characters ***** and **?** when issuing the **delete** command.

Caution: You cannot recover a file after it is deleted. The **delete** command does not prompt you to verify a deletion.

Enter the following to delete a file in the present working directory:

delete *<filename>*

You can enter **del** or **delete** when deleting a file.

Note: You cannot delete a file whose attributes are **h** (for hidden) or **s** (for system). Refer to "Changing File Attributes," earlier in this chapter, for instructions on changing these protections.

Examples:

If you enter:	The system:
delete alt.cfg	Deletes the *alt.cfg* file in the present working directory.
delete *.log	Deletes all files with the *log* filename extension in the present working directory.
delete ???.log	Deletes all files with a three-character filename and a *log* filename extension.

Chapter 6
Managing Events

You can use the Technician Interface to

- Specify events you want to include in, or exclude from, the events log
- Specify events you want to display from the events log
- Save an events log to a file
- Configure the router to save the events log to a new file automatically when the log becomes full
- Display an events log file previously saved
- Clear event messages from the events log

Refer to *Event Messages for Routers and BNX Platforms* for information about the event display format or about specific events.

Overview

The operating software in each processor module logs (stores) events in a first-in, first-out (FIFO) memory buffer.

When you issue a command to display or save the current log, the system sorts the events from all processor modules in chronological order. You can also clear events from all slots or from a single slot.

The event logs are checksum protected during a warm start. (Issuing the **boot** or **reset** command or pressing the Reset button warm-starts the router.) However, events are lost during a cold start. (Power-cycling the router or issuing the **diags** command cold-starts the router.) When you remove and reinsert a processor module, the events clear from that module only.

Logging and Displaying Event Messages

Use the **log** command mainly to specify the types of events that you want the router to include in the events log, exclude from the events log, or display from the events log, as follows:

- To display the unfiltered contents of the events log, enter the **log** command without any command arguments.
- To select the types of messages you want the router to include in, or exclude from, the events log, add *write filter* arguments to the **log** command. You can select or specify event types by
  - -- Entity code
  - -- Message severity levels
  - -- Router slot numbers
- To display all write filters currently in effect, enter the **log** command with the **-z** subcommand option.

- To enable the router to read only certain messages from the events log to the console display, add *read filter* arguments to the **log** command. You can select or specify event types by
  - -- Entity code
  - -- Severity level
  - -- Slot number
  - -- Event date
  - -- Event time
  - -- Event number or number range

Applying Write Filters to the Events Log

During normal operation, the events log captures all event messages generated internally by the router. However, *for troubleshooting purposes only*, use the **log** command to

- Include specific event messages in the events log.
- Exclude specific event messages from the events log.

Specify the **log** command as follows:

log [**-i** | **-x**] [**-e***<entity>*] [**-f***<severity>*] [**-s***<slot_ID>*]

-i = Include the **-e**, **-f**, and/or **-s** options that follow.

-x = Exclude the **-e**, **-f**, and/or **-s** options that follow.

Note: You can add the **-e**, **-f**, and **-s** arguments to the **log** command in any order.

After log -i or log -x, enter:	Followed by:	To specify:
-e	*<entity_name>*	The name of the software service for which the router will log (write) event messages to the local events log, or exclude from the events log. When you specify an <entity_name>, you must • Use uppercase letters. • Enter the <entity_name> in quotes when that name contains spaces (for example, “FRAME RELAY”). See *Event Messages for Routers and BNX Platforms* for a list of router software entity names.
-f	*<severity_levels>*	The severity levels of messages that the router will log (write) to the local events log, or exclude from the events log. The severity codes are • f or F for fault • i or I for informational • t or T for trace • w or W for warning • d or D for debug (Debug events are for use and interpretation by Bay Networks Technical Response Center personnel only.) You can specify in the same log command one or more severity codes. For example, enter **log -i -fwi** to specify a filter that writes only Warning and Info messages to the events log.
-s	*<slot_numbers>*	The number of the slot(s) on which the router will write event messages to the local log buffer.

Examples:

If you enter:	The events log:
log -i -fdft	Includes only debug, fault, and trace events
log -i -fdi -s2	Includes only debug and info events on slot 2
log -i -ff -eGAME	Includes only fault events for the router operating system entity,
log -i -fd -s2 -eOSPF	Includes only debug events for OSPF running on Slot 2
log -i	Includes no events (since none are specified)
log -i -fdfitw	Includes all events (since all severity levels are specified)
log -x -fd	Excludes only debug events
log -x -fdfitw -eIP	Excludes all except IP events
log -x	Excludes no events (since none are specified)
log -x -fdfitw	Excludes all events (since all severity levels are specified)

Displaying Active Write Filters

Display a list of all write (log input) filters currently in effect across the router, as follows:

If you enter:	The Technician Interface:
log -z	Displays write filters currently in effect across all slots.
log -z [**-s***<slot>*]	Displays write filters currently in effect for the slot you specify.

Applying Read (Display) Filters to the Events Log

Enter the following command to display the events stored in all event buffers.

log

The system sorts the events and displays them in chronological order. For information about the event display format or about specific events, refer to the guide *Managing Routers and BNX Platforms*.

Note: To abort the command, press control-c (hold the control key and press c).

Add arguments to the **log** command to select the event types you want to display. Enter the log command as follows, to limit the display of events:

log [<*vol*>:<*log_file*>] [**-d**<*date*>] [**-t**<*time*>] [**-e**<*entity*>] [**-f**<*severity*>] [**-s**<*slot_ID*>] [**-p**<*rate*>] [**-c**<*code_no.*>] [**-w**]

You can enter any combination of the following optional parameters:

<*vol*>:<*log_file*> is the volume number or letter where a log file is located, and the name of the log file. The system displays the events saved to this file.

<*date*> is the date in mm/dd/yy format. The system displays the events logged on and after that date.

<*time*> is the time in hh:mm:ss format. The time you can enter ranges from 00:00:00 to 23:59:59. The system displays the events logged at and after that time.

<*entity*> is a software service that logs events. Quotes are required when the <*entity*> contains spaces. Use uppercase letters when specifying the <*entity*>. See *Event Messages for Routers and BNX Platforms* for a list of the entities.

<*severity*> is one or more letter codes for an event type. The system displays the events by type. The severity codes are **f** or **F** for fault, **i** or **I** for informational, **t** or **T** for trace, **w** or **W** for warning, and **d** or **D** for debug. (Debug events are intended only for Bay Networks Technical Response Center personnel.)

<*slot_ID*> is the number of the slot containing a link module. The system displays the events associated with the link module.

<*rate*> is an option that enables continuous polling of the system's events log and display of new event messages. **-p** uses a default rate of 5 seconds. You can change this by entering a <*rate*> in seconds. The system displays the events that occur between polling intervals.

<*code_no.*> is an event code number or a range of event code numbers. The system displays the events associated with the specified event code.

-w enables the **log** command to provide console output in wide format.

Examples:

If you enter:	The console displays:
log	All fault, warning, and info events in memory.
log 3:ftp.log	All events saved to the *ftp.log* file stored on Volume 3.
log -d12/12/94	Displays all events logged since December 12, 1994.
log -t09:02:00	All events logged since 9:02 today. If it is earlier than 9:02, the console displays all events logged since 9:02 yesterday.
log -eTFTP	All events logged by the TFTP service.
log -eGAME -eTI	All events logged by the GAME and TI services.
log -ffw	All fault and warning events.
log -s3	All events logged in Slot 3.
log -eTFTP -ffw -s3	All fault and warning events logged by the TFTP service in Slot 3.
log -eTCP -eTELNET -ffw	All fault and warning events logged by the TELNET and TCP services.
log -p10	All events logged in the past 10 seconds.
log -c8	All events associated with Event Code 8.
log -w	All events in wide format, as follows:

Example (log -w)

```
#1: 08/13/95 16:32:20.011  INFO  SLOT  2  GAME  Code:11  Starting image int/9.00/52 Mon Jul 31 22:20:19 EDT
#2: 08/13/95 16:32:21.031   INFO  SLOT  2  GAME  Code:9   BackBone 0 became re-connected
#3: 08/13/95 16:32:21.511   INFO  SLOT  2  GAME  Code:10  slot  4 became re-connected
#4: 08/13/95 16:32:21.554   INFO  SLOT  2  GAME  Code:10  slot  3 became re-connected
#5: 08/13/95 16:32:29.238   INFO  SLOT  2  NVFS  Code:42  Volume 2: Service initializing.
#6: 08/13/95 16:32:33.347   INFO  SLOT  2  MIB   Code:4   Using configuration file '2:config'
#7: 08/13/95 16:32:33.480   INFO  SLOT  2  MIB   Code:3   Service initializing.
```

Saving the Events Log

You can save the events in the current event buffer to a file for later retrieval.

Caution: The system automatically overwrites any file on the volume that has the same filename. To avoid overwriting an existing file, display a list of the volume's contents (with the **dir** *<vol>***:** command) and determine the filenames already in use.

Enter the following.

save log *<vol>***:***<log_file>*

<vol> is the volume on which to store the file

<log_file> is the name of the file you are creating to store the events.

We recommend that you use the *.log* file extension when creating log files.

You can verify that the log file is saved by entering the **dir** *<vol>***:** command.

You can use the same optional arguments when displaying a log file you previously saved, as you can to display a current log (refer to the section that follows for instructions).

Another option is to limit the event types you save to a log file. When you display the log file after saving it, only those event types you saved are displayed. Enter the following command to limit the event types you save to a log file:

save log *<vol>***:***<log_file>* [**-d***<date>*] [**-t***<time>*] [**-e***<entity>*] [**-f***<severity>*] [**-s***<slot_ID>*]

Refer to the previous section for a description of the optional arguments.

Note: The **save log** command does not clear events from memory. Refer to "Clearing Events," later in this chapter.

Examples:

If you enter:	The system saves:
save log 2:10_12.log	All events to a file named *10_12.log* in Slot 2.
save log 2:10_12.log -d10/12/95	Events logged since October 12, 1995 to a file named *10_12.log* in Slot 2.
save log 2:temp.log -t09:02:00	Events logged since 9:02 today to a file named *temp.log* in Slot 2. If it is earlier than 9:02, the system saves all events logged since 9:02 yesterday.
save log 3:tftp.log -eTFTP	Events logged by the TFTP driver to a file named *tftp.log* in Slot 3.
save log 3:snmp.log -eSNMP -ftf	Trace and fault events logged by the SNMP driver to a file named *snmp.log* and stores the file in Slot 3.
save log 2:slot3.log -s3	Events logged in Slot 3 to a file named *slot3.log* and stores the file in Slot 2.

Saving the Events Log Automatically

Note: Use this feature only for the purpose of troubleshooting a Bay Networks router. Leave the feature disabled (by default) at all other times.

You can configure any model of Bay Networks router to save the entire events log automatically. The system saves the file just prior to overwriting the oldest messages in the log. This feature helps to prevent the loss of event message information accumulated in the log over time.

The system

- Saves the log the number of times you designate in MIB attribute wfSerialPortEntry.wfSerialPortAutoSaveNumFiles (or until the memory card or diskette drive becomes full)
- Saves the log to the memory card or diskette file system volume you designate in MIB attribute wfSerialPortEntry.wfSerialPortAutoSaveVolume
- Saves the log to the filename *auto<x>.log*, where *<x>* is a value from 1 to the maximum value you set for MIB attribute wfSerialPortEntry. wfSerialPortAutoSaveNumFiles

Parameter:	**Maximum Autosaved Files**
Attribute Name:	wfSerialPortAutoSaveNumFiles
Attribute Name:	33
Default:	0 (log autosave off)
Options:	0 to 99
Function:	Specifies the number of times the system automatically saves the events log to a file system volume. The system saves the log the maximum number of times you specify, or until the memory card or diskette drive on the router becomes full.
Instructions:	Accept the default value (0, disabled) or specify the number of times you want to save the log to a new file.
Command:	**set wfSerialPortEntry.33.***<instance_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.33

Parameter:	**Autosave Volume**
Attribute Name:	wfSerialPortAutoSaveVolume
Attribute Name:	34
Default:	None
Options:	Any valid memory card volume (slot) number from 1 to 14 (or) the diskette drive designation, **-a**
Function:	Specifies the target volume where the system stores new log files saved through the log autosave feature.
Instructions:	Specify the memory card or diskette file system volume where the system will save log files automatically through the log autosave feature.
Command:	**set wfSerialPortEntry.34.***<instance_no.> <option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.11.1.1.34

Log Autosave Platform Differences

This section describes platform-specific differences you need to consider before attempting to configure the log autosave feature on any Bay Networks router.

Models AFN, ALN, AN, ANH, BLN, BLN-2, BCN, and BNX -- Each model supports only one instance of the wfSerialPortEntry object. For that instance, you can configure the log autosave attributes wfSerialPortAutoSaveNumFiles and wfSerialPortAutoSaveVolume.

Models CN, FN, and LN -- Each model supports 4 instances of the wfSerialPortEntry object. Each instance corresponds to one of the following *ports*:

- wfSerialPortEntry.wfSerialPortName.1 = "CONSOLE"
- wfSerialPortEntry.wfSerialPortName.2 = "MODEM1"
- wfSerialPortEntry.wfSerialPortName.3 = "MODEM2"
- wfSerialPortEntry.wfSerialPortName.4 = "PRINTER"

Configure the log autosave attributes for the “CONSOLE” port instance only.

Model ASN -- Supports 4 instances of the wfSerialPortEntry object. Each instance corresponds to one of the 4 slots possible in an ASN stack. Enable the log autosave feature only on one occupied slot in the ASN stack.

Models 5380 and 5580 -- System 5000 hubs support up to 14 instances of the wfSerialPortEntry object. Each instance corresponds to one of the 14 possible hub slots. Enable the log autosave feature only on one slot occupied by a Model 5380/5580 router in a System 5000 hub. (Multiple 5380/5580 boards installed in the same System 5000 hub operate as one logical router if that hub contains an ATM/PPX backplane.)

Note: If the System 5000 does not contain an ATM/PPX backplane, each Model 5380/5580 board operates as an independent router. In this case, you can configure the log autosave feature on each Model 5380/5580 board independently.

Configuring the Log Autosave Feature

Proceed as follows to enable and customize operation of the log autosave feature:

1. **Determine how you want to configure the log autosave feature, based on descriptions of**
   - **wfSerialPortEntry attributes *wfSerialPortAutoSaveNumFiles* and *wfSerialPortAutoSaveVolume***
   - **Log autosave platform differences (see previous section)**
2. **Open a Technician Interface session with the router.**
3. **Enter with appropriate arguments the command shown for each attribute, followed by a commit command**
4. **Close the Technician Interface session when you finish configuring the log autosave feature.**

Repeat this procedure for any Bay Networks router on which you need to enable the log autosave feature.

For more explanation of the Technician Interface **set** and **commit** commands, refer to “Using the Set Command” and “Using the Commit Command” in Chapter 2.

Displaying an Events Log File Previously Saved

You can use the **log** command to display a log file you previously saved. Enter the following to display a log file, where <*vol*> identifies the volume and <*log_file*> is the name of the log file you want to display:

log [<*vol*>**:**<*log_file*>]

The system reads the log file, which is stored in binary, and forwards an ASCII representation to the console.

The event format is identical to the format of the current log display.

You can use the same optional arguments when displaying a log file as you can to display or save the current log. Enter the following command to limit the event types to display:

log <*vol*>**:**<*log_file*> [**-d**<*date*>] [**-t**<*time*>] [**-e**<*entity*>] [**-f**<*severity*>] [**-s**<*slot_ID*>]

Refer to "Logging and Displaying Event Messages," earlier in this chapter, for a description of the optional arguments.

Examples:

If you enter:	The console displays:
log 2:10_12.log	All events stored in the *10_12.log* file in Slot 2.
log 2:10_12.log -eTFTP	All events logged by the TFTP driver and stored in the *10_12.log* file in Slot 2.
log 2:10_12.log -eSNMP -ftf	All trace and fault events logged by the SNMP driver and stored in the *10_12.log* file in Slot 2.
log 2:10_12.log -s3	All events logged to Slot 3 and stored in the *10_12.log* file in Slot 2.

Clearing Events

Clearing events from the events log buffer is useful if you want to conduct an experiment and examine the events log afterwards.

Note: You may want to save the log to a file for later retrieval before clearing it. (Refer to "Saving the Events Log," earlier in this chapter.)

Enter the **clearlog** command with one or more of the following parameters to clear all events from an event buffer or buffers. <*slot_no.*> is the location of the log buffer you are clearing.

clearlog [<*slot_no.*>]

clearlog [<*slot_no.*>-<*slot_no.*>]

clearlog [<*slot_no.*>,<*slot_no.*>. . .]

The system automatically clears all events from the buffer associated with the slot or slots you indicate.

Examples:

If you enter:	The system clears all events from:
clearlog	Memory.
clearlog 2	The Slot 2 event buffer.
clearlog 5-7	The Slot 5, 6, and 7 event buffers.
clearlog 2,5,8	The Slot 2, 5, and 8 event buffers.

Chapter 7
Accessing the MIB

You can use the Technician Interface to access and manage the Bay Networks Management Information Base (MIB). This chapter assumes you already know how to manage the MIB, but you need instructions on entering MIB management commands at the Technician Interface console. Refer to Appendix A for more information.

You can manage the Bay Networks MIB as follows:

- Display MIB object names, identifiers, and values
- Change MIB values
- Commit MIB value changes
- Save the configuration in RAM to a file for later retrieval when booting
- Use the MIB-II counter

Listing MIB Objects

You can display MIB object names and their associated identifiers using the **list** command. When you want to display or change a MIB value but don't know its object or attribute name, use this command.

Enter the following to display a list of all MIB object names and identifiers:

list

You can also enter the following to display a list of attributes and their associated identifiers, where [<*object_name*>] is the name of the object at the level above the attributes:

list [<*object_name*>]

Finally, you can display a list of instance identifiers using the **list** command. Enter the **list** command with the following parameters to display a list of instance identifiers:

list [[**instances**] [<*object_name*>]]

or

list [[**-i**] [<*object_name*>]]

[**instances**] or [**-i**] represents the optional key word **instances**.

[<*object_name*>] is the name of the object at the level above the attributes.

Examples:

If you enter:	The console displays:

list	All object names and their associated object identifiers:
	`wfCSMACDEntry = 1.3.6.1.4.1.18.3.4.1.1`
	`wfFddiEntry = 1.3.6.1.4.1.18.3.4.4.1`
	`wfFddiSmtEntry =`
	`1.3.6.1.4.1.18.3.4.15.1.21`
	.
	.
	.

list wfCSMACDEntry	All attribute names and associated attribute identifiers of the wfCSMACDEntry object:
	`wfCSMACDDelete = 1`
	`wfCSMACDEnable = 2`
	`wfCSMACDState = 3`
	.
	.
	.

list instances wfCSMACDEntry
list -i wfCSMACDEntry
	All instance identifiers of the wfCSMACDEntry object configured on your system:
	`inst_ids = 2.1`
	`2.2`
	`4.1`
	`4.2`

Getting MIB Values

The **get** command displays the value of a MIB object. You can also insert a wildcard character (*****) into the attribute name *or* into the instance identifier to display the values of multiple objects.

Enter the following to display one or more object identifiers and their associated values:

get *<object>.<attribute>.<instance>*

or

g *<object>.<attribute>.<instance>*

<object> is the required object name or identifier.

<attribute> is the required name, identifier, or wildcard character of the object attribute(s). The wildcard character * displays all attributes of the object and their associated values.

<instance> is the optional name or identifier of the instance. An asterisk (*) in place of the instance displays all instances of the object and their associated values. You can also indicate an asterisk as part of the instance identifier to display all instances that begin with the partial instance you specify. For example, if you enter the following command, the system returns all instances of Attribute 1, wherever the instance ID also begins with 192.32.

get wfIpBaseRtEntry.1.192.32.*

Note: You cannot use more than one wildcard in a **get** command.

The following examples demonstrate ways to display the value of an attribute. The attribute in these examples is named wfSnmpDisable. Its instance ID is 1. Its object name is wfSnmp and object identifier is 1.3.6.1.4.1.18.3.5.3.5.1.

The instance ID of 0 is reserved for base record objects. Specifying the base record instance ID in the **get** command is optional. (Refer to the second example.)

The last example demonstrates how to obtain a group of values associated with an object.

Examples:

If you enter:	**The console displays:**
Any one of the following: **get wfSnmp.wfSnmpDisable** **get wfSnmp.wfSnmpDisable.0** **get 1.3.6.1.4.1.18.3.5.3.5.1.1** **get 1.3.6.1.4.1.18.3.5.3.5.1.1.0** **get 1.3.6.1.4.1.18.3.5.3.5.1.1.*** **get wfSnmp.1.0** **get wfSnmp.1.***	`wfSnmp.wfSnmpDisable.0 = 1` (The object name, the base record (0), and the value.) Appending the base (0) to the object name is optional when issuing a **get** command. Likewise, appending the base (0 or *) to the instance identifier is optional when issuing a **get** command.

get wfSnmp.*.0	`wfSnmp.wfSnmpDisable.0 = 1`
	`wfSnmp.wfSnmpUseLock.0 = 1`
	`wfSnmp.wfSnmpLockAddress.0 = 0.0.0.0`
	`.`
	`.`
	`.`

get wfSnmp.*.*	`get: Invalid obj.attr.inst specified`

Setting MIB Values

The **set** command modifies the value of an instance. You set an instance by specifying its *object.attribute.instance*. You may use names or identifiers to specify object groups and attributes; use only an appropriate identifier or index value to specify the instance.

Note: When you enter the **set** command, the attribute is set on each running processor module.

Enter the following to change the value of an object instance:

set *<object>.<attribute>.<instance> <value>*

or

s *<object>.<attribute>.<instance> <value>*

<object> is the required name or identifier of the object.

<attribute> is the required name or identifier of the attribute.

<instance> is the required unique identifier of a nontabular object, or the "INDEX" value of a tabular object.

Note: The MIB uses the value of the "INDEX" in the "Entry" (.1) attribute of a **table object** to define the *<instance_id>* of any entry belonging to that table. The INDEX typically defines the *<instance_id>* by means of one attribute, or by means of multiple attributes that together define the *<instance_id>* of a table entry.

<*value*> is the required new value of an instance of an object. This value may be one of the following, depending on the data type:

- Integer, unsigned integer types: decimal number
- IP addresses: dotted decimal format (for example, 192.32.0.0)
- Octet strings: hexadecimal number starting with 0x
- Display strings: string enclosed in double quotes

Refer to the Bay Networks MIB to determine the data type.

Caution: If you are running Spanning Tree, always follow any Technician Interface **set** command to the Bridge with the corresponding Technician Interface **set** command to the Spanning Tree. Otherwise, you may lose connectivity to LANs. Refer to the last two examples that follow.

Also, make sure the values you set are legal. Illegal or incompatible MIB values can disrupt software or network services after you enter the **commit** command. Refer to the Bay Networks MIB for the legal values.

You can use the **list** command or refer to the Bay Networks MIB to determine the symbolic names and identifiers for object groups and attributes.

Use the **commit** command (described in the next section) to notify the software services of the MIB changes accomplished with the **set** command. Then, to copy the changes you make to a configuration file, use the **save** command (described in "Saving the Configuration").

Note: Be sure to enter **commit** after entering the **set** command (see the next section for instructions).

Examples:

If you enter:	The system:
Any one of the following:	
set wfSnmp.wfSnmpDisable.0 1 **set 1.3.6.1.4.1.18.3.5.3.5.1.1.0 1** **set wfSnmp.1.0 1**	Changes the value of wfSnmp.wfSnmpDisable.0 (1.3.6.1.4.1.18.3.5.3.5.1.1.0) to 1 to enable SNMP.
set wfIpInterfaceEntry.2.192.32.13.99.32	Changes the value of wfIpInterfaceEntry.WfIpInterfaceEnable.192.32.13.99 to 2. This disables IP for the interface whose IP address is 192.32.13.99 and whose circuit is 3.
Both of the following: **set wfBrTp.2.0 1** **set wfBrStp.2.0 1**	Changes the values wfBrTp.wfBrTpBaseEnable.0 and wfBrStp.wfBrStpBaseEnable.0 to 1 to enable the Translating Bridge and Spanning Tree.
Both of the following: **set wfBrTp.2.0 2** **set wfBrStp.2.0 2**	Disables the Translating Bridge and Spanning Tree.

Committing MIB Sets

The **commit** command causes all previously entered **set** commands to take effect. When you enter **commit**, the system notifies all software services whose configuration parameters have changed.

Refer to the following section to copy all MIB values from operating RAM to a configuration file for later retrieval.

Saving the Configuration

You can copy all MIB values from operating RAM to a configuration file for later retrieval. You use the **save config** command to copy the configuration in memory to the default configuration file or to an alternative configuration file. Enter the following, where <*filename*> is the name of the file you are creating to store the configuration:

save config <*vol*>:<*filename*>

Examples:

If you enter:	The system:
save config 2:config	Overwrites the default configuration file *config* on Volume 2 with the configuration in memory.
save config 2:config.2	Creates an alternate configuration file named *config.2* on Volume 2 and stores the configuration residing in memory in this file.

Refer to "Booting the Router" in Chapter 8 to load a configuration from a file.

Using the MIB-II Counter

You can use the MIB-II counter feature with Version 8.10 and later router software. The feature enables you to track the number of packets each circuit in the Bay Networks router processes at the data link layer.

You can enable the Bay Networks MIB to count all incoming and outgoing packets by using the **set** and **commit** commands with the following parameter.

Parameter:	**MIB II Counters Enable**
Attribute Name:	wfSysMibCounterEnable
Attribute Number:	12
Default:	1 (Enable)
Options:	1 (Enable) | 2 (Disable)
	Enables or disables the following five counters in the MIB for Version 8.10 and later router software: – ifInUcastPkts – ifInNUCastPkts – IfINUnknownProtos – ifOutUcastPkts – ifOutNUcastPkts
Instructions:	Set to 1 (Enable) to enable the five counters on all circuits and slots. Set to 2 (Disable) to disable the counters on all circuits and slots.
Command:	**set wfSys.12.0** *<option>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.1.12

Chapter 8
System Administration

You can use the Technician Interface to perform the following system administration tasks:

- Configure the Access Node (AN) or Access Stack Node (ASN) router's boot or configuration sources when booting
- Configure AN or ASN initial interfaces
- Boot the router
- Configure and manage delayed boot services
- Restart a slot
- Reset a slot
- Run diagnostics
- Display the version number of the Bay Networks router software
- Halt the transfer of packets between slots
- Verify and upgrade the software
- Validate an executable file
- Upgrade and verify a PROM
- View the address and size of a dynamically loadable application
- Set the Bay Networks ACE backplane type
- Reset the date and time
- Assign Technician Interface passwords

- Enable/disable SecurID authentication
- Manage Secure Mode
- Configure search depth for hardware compression
- Display a greeting or message before the login prompt
- Customize the Technician Interface Welcome message
- Record console messages to a file
- Enable Internal Clocking Mode
- Respond to QENET Underflow Errors
- Monitor IP routes (for IP, OSPF, BGP)

A table of all the Technician Interface commands and their associated access levels appears at the end of this chapter (Table 8-4).

AN/ANH/ASN Administration

The following sections apply to the Access Node (AN), Access Node Hub (ANH), and Access Stack Node (ASN) routers. The following guides collectively provide complete instructions for setting up Netboot and Directed Netboot on an AN, ANH, or ASN router:

- *Installing and Operating BayStack AN and ANH Systems*
- *Installing and Maintaining ASN Routers and BNX Platforms*
- *Connecting BayStack AN and ANH Systems to a Network*
- *Connecting ASN Routers and BNX Platforms to a Network*

You need to use the **ifconfig** and **bconfig** commands to configure the AN, ANH, and ASN:

- Use the **ifconfig** command to configure the router's initial IP interface to the network.
- Use the **bconfig** command to specify the location and name of the router's software image and configuration file.

Configuring the Boot Source

To use Directed Netboot, you must use the **bconfig** command to specify the following:

- The IP address of the server where the router's software image and/or configuration file reside.
- The full pathname of the software image and configuration file.

You must use the **bconfig** command once to specify the location of the software image, and again to specify the location of the configuration file.

Use one of the following formats for the **bconfig** command:

bconfig [**image** | **config**] [**local** | **network** [*<TFTP_host> <TFTP_pathname>*]]

bconfig -d [**image** | **config**]

Note: After making the change, enter the following command to save it to the configuration file in the router's file system, as follows:

save config 1:config

config is the name of the configuration file.

Table 8-1 describes command settings for the **bconfig** command:

Table 8-1. bconfig Command Settings

Option	Description
image	Specifies information about the router's software image.
config	Specifies information about the router's configuration file.
local	Indicates that the specified file (image or config) resides in the router's local file system.
network	Indicates that the specified file resides on a network server.

Table 8-1. bconfig Command Settings *(continued)*

Option	Description
<TFTP_host>	Specifies the IP address of the host where the image or configuration file resides. If both the software image and configuration file reside on the network, the files must reside on the same host. In other words, you must specify the same IP address for the TFTP host for both files.
<TFTP_pathname>	Specifies the complete pathname of the software image or configuration file on the host.
-d	Resets the default values for the software image or configuration file. The command **bconfig -d image** tells the router to look for the image file locally, and nullifies the IP address and pathname for the file. The command **bconfig -d config** tells the router to obtain the configuration file over the network, and nullifies the IP address and pathname for the file. Without the IP address and pathnames, the router resorts to using Netboot rather than Directed Netboot. However, if you want to get one file locally while using Directed Netboot for the other file, you can use the **bconfig** commands as the following examples show: **bconfig image local** **bconfig config network 21.3.5.62 /usr/anstartup/config** or **bconfig image network 21.3.5.62 /usr/mykernel.exe** **bconfig config local**

Configuring Initial Interfaces and Netboot Operation

You can use the **ifconfig** command to do the following:

- Configure the router's initial IP interface to the network. You also use the same procedure to configure other synchronous interfaces for the network booting procedure.
- Configure Ethernet interfaces for the network booting procedure.
- Enable or disable network booting on an interface.

The following sections describe each use of the **ifconfig** command.

Configuring the Initial IP Synchronous Interface

To Netboot the router, you must first configure the router's initial IP synchronous interface to the network, using the following interface configuration command:

ifconfig [**-s***<slot_no.>*] *<synchronous_options> <interface>* [*<IP_address> <subnet_mask>* [*<next_hop_address>*]]

<synchronous_options> indicates some combination of the following settings:

[**-d** | **-fr** [**-annexd** | **-lmi** | **-annexa**] | **-int_clk**]

Note: You must insert a space to separate each command option from the next.

You can use the same command format to configure other synchronous interfaces on the router for network booting.

Table 8-2 describes the **ifconfig** command arguments for configuring a router's synchronous interface.

Table 8-2. ifconfig Command Settings

Setting	Description
Slot setting:	
-s<*slot_no.*>	Specifies the slot containing the interface you want to configure. The slot corresponds to the ASN slot ID, which can be 1 through 4. If you omit this argument, **ifconfig** uses the current slot.
Default setting:	
-d	Resets the router's IP interface settings to the default values. This setting tries four WAN configurations in the following order until it finds the correct type for the router's connection to the network: 1. Bay Networks HDLC encapsulation (also referred to as Bay Networks Standard Point-to-Point) with external clocking 2. Frame Relay Annex D 3. Frame Relay LMI 4. Frame Relay Annex A
Frame Relay settings:	
-fr	Configures the router's synchronous port as a Frame Relay connection. With this setting, use one of the following options to specify a DLCMI setting: **-annexd**, **-annexa**, or **-lmi**.
-annexd **-annexa** **-lmi**	When one of these options is used with the **-fr** setting, it specifies a DLCMI setting. Use the same setting as the network to which the router's Frame Relay interface is connected. The default setting for Frame Relay is **-annexd**.
Internal clocking setting:	
-int_clk	Sets the router's synchronous port to internal clocking at 1.25 MB/s. If you do not specify the **-int_clk** setting, the router defaults to external clocking.
IP connector setting:	
<interface>	Specifies the type of IP connector you are configuring. For the AN and ANH, use **com1** or **com2** for synchronous media. For the ASN, use **com**<*network_module_no.*><*port_no.*>.

(continued)

Table 8-2. ifconfig Command Settings *(continued)*

Setting	Description
IP address settings:	
<IP_address>	Specifies the IP address of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<subnet_mask>	Specifies the IP subnet mask of the interface you selected with the *<interface>* setting. Provide this address in dotted decimal notation.
<next_hop_address>	Specifies the IP address of the next-hop router. Provide this address in dotted decimal notation. You only need to specify this address if there are intermediate routers between the router and the BOOTP server.

Configuring an Ethernet Interface for Network Booting

To configure an Ethernet interface for network booting of a router, use the following command format:

ifconfig [**-s***<slot_no.>*] [**-d**] *<interface>* [*<IP_address>* *<subnet_mask>* [*<next_hop_address>*]]

Table 8-3 describes the **ifconfig** command arguments for configuring the router's Ethernet interface.

Table 8-3. ifconfig Settings for an Ethernet Interface

Setting	Description
Slot setting:	
-s*<slot_no.>*	Specifies the slot containing the interface you want to configure. The slot corresponds to the ASN slot ID, which can be 1 through 4. If you omit this argument, **ifconfig** uses the current slot.
Default setting:	
-d	Resets the router's IP interface settings to the default values. Resetting an Ethernet interface makes it inactive in the network booting process. (The output of the **getcfg** command shows the default as "None.")
IP connector setting:	
<interface>	Specifies the type of IP connector you are configuring. For the AN and ANH, use **xcvr1**. For the ASN, use **xcvr***<network_module_no.><port_no.>*.

(continued)

Table 8-3. ifconfig Settings for an Ethernet Interface *(continued)*

Setting	Description
IP address settings:	
<IP_address>	Specifies the IP address of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<subnet_mask>	Specifies the IP subnet mask of the interface you selected with the *<interface>* setting. Provide this address in dotted decimal notation.
<next_hop_address>	Specifies the IP address of the next-hop router. Provide this address in dotted decimal notation. You only need to specify this address if there are intermediate routers between the router and the BOOTP server.

Enabling and Disabling Interfaces with ifconfig

To enable an AN or ANH interface for the network boot process or to disable an interface from the network boot process, use the following command formats:

ifconfig -disable *<interface>*

ifconfig -enable *<interface>*

To enable an ASN interface for the network boot process or to disable an interface from the network boot process, use the following command formats:

ifconfig [**-s***<slot_no.>*] **-disable** *<interface>*

ifconfig [**-s***<slot _no.>*] **-enable** *<interface>*

<slot_no.> Specifies the slot containing the interface you want to enable or disable. The slot corresponds to the ASN slot ID, which can be 1 through 4. If you omit this argument, **ifconfig** uses the current slot.

<interface> Specifies the type of IP connector you are enabling or disabling. For the AN and ANH, use **com1** or **com2** (for synchronous media) or **xcvr1** (for Ethernet media).

For the ASN, use

xcvr *<network_module_no.> <port_no.>*

or

com *<network_module_no.> <port_no.>*

Booting the Router

The Technician Interface provides the following commands for booting:

- The **boot** command warm-starts the entire system. Pressing the Reset button on the front panel of the router initiates the same procedure.

  You can override the default router software image and configuration by specifying an alternative router software image and an alternative configuration file when entering the **boot** command.

- The **reset** command warm-starts a single processor module or the entire system with the router software image and configuration currently in use. Resetting the entire system is equivalent to booting it.

- The **diags** command cold-starts a single processor module or the entire system. The cold start consists of CPU, backbone, and link diagnostics, and a reboot. If you do *not* enter a slot number, the system tests and reboots all slots.

How the Router Boots

This section describes how each processor module in the router obtains its router software image and configuration when you do *not* override the default router software image (for example, *bn.exe*) and configuration file (*config*).

You do *not* override these files when you

- Power-cycle the router
- Issue the **diags** command
- Hot-swap a module
- Issue the **reset** command
- Issue the **boot** command without specifying defaults

A cold start occurs when you power-cycle the router or issue the Technician Interface **diags** command. The processor module executes CPU and backbone diagnostics, and if a link module is present, link diagnostics. When CPU and backbone diagnostics terminate successfully, and link diagnostics terminate (successfully or unsuccessfully), the processor module boots.

A warm start occurs when you hot-swap a module, press the Reset button, or issue the **boot** or **reset** command. The processor module boots without running diagnostics. When you hot-swap a module, the DIAG LED on the front panel and LED 8 on the FRE module daughterboard behind the RFI shield remain on, indicating that diagnostics have not been run. (We recommend that you issue the **diags** command when you hot-swap a board.)

When a processor module boots, it requests a copy of the router software image currently in use. The first processor module to respond to the request forwards a copy of the router software image from its memory. If none is in use, the processor module uses the router software image stored on its own volume, if one is available. The processor module then boots.

The processor module requests a copy of the configuration currently in use after it boots. The first processor module to respond to the request forwards a copy of the configuration from its memory. If none is in use, the processor module uses the default configuration file (*config*) stored on its own volume, if one is available. The processor module then loads the configuration and initiates software services.

Booting

Use the **boot** command to boot the entire system.

Caution: If you do not specify the router software image and configuration file when entering the **boot** command, the system boots from the default image (for example, bn.exe) and configuration file (config). We recommend that you have only one version of the config file on the router. You can comply with this recommendation by assigning new names to alternative versions of the configuration file. It is possible that the processor modules can simultaneously load different configurations if you have alternative versions of the config file and you enter the **boot** command without specifying the volume and configuration file with which to boot.

Enter the following command to boot the entire system with the default software image (for example, *bn.exe*) and default configuration file (*config*).

boot

You can also boot the entire system by naming a specific image or configuration file. With this “named boot” operation, the system uses the image or config file name that you specify instead of the default image or config file. Use the following syntax to perform a named boot operation:

boot *<vol>*:*<image_name>* *<vol>*:*<config_name>*

boot *<vol>*:**-** *<vol>*:*<config_name>*

boot *<vol>*:*<image_name>* *<vol>*:**-**

<vol> identifies the volume that contains the *<image_name>*. *<image_name>* identifies the filename of the router software image, or “ **-** ” identifies the default router software image.

<vol> identifies the volume that contains the *<config_name>*. *<config_name>* identifies the name of the configuration file, or “ **-** ” identifies the default configuration file (*config*).

Note: If you enter one argument in the **boot** command, you must enter the other. If you want to use the default router software image with a named configuration file, you must enter a dash (**-**) as the image argument. Similarly, to use a named router software image with the default configuration file, you must enter a dash (**-**) as the configuration argument. When the source is network, enter only a dash (**-**) to indicate no volume for the router software image or config. If you enter anything else, the Technician Interface displays an error message.

The software image and configuration files revert to their respective default filenames (*ace.out*, *an.exe*, *afn.exe*, *asn.exe*, *bn.exe*, or *config*) after every boot. To change the default boot or configuration file, overwrite the old default file with the new default file, using the **copy** command. But be sure to back up the old default file, using the **copy** command, before overwriting it.

Examples:

If you enter:	The system boots with:
boot	The default router software image (for example, *bn.exe*) and the configuration file (*config*) on the volume to come up with the valid boot name.
boot 2:- 2:- or **boot 2:bn.exe 2:config**	• The (default) router software image on Volume 2 The (default) configuration file (*config*) on Volume 2
boot 2:net1.exe 3:-	• The *net1.exe* router software image on Volume 2 • The (default) configuration file (*config*) on Volume 3
boot 3:- 2:Trident.cfg	• The default router software image on Volume 3 • The user's customized configuration file *Trident.cfg* on Volume 2
boot 2:net1.exe 2:Trident.cfg	• The *net1.exe* router software image on Volume 2 • The user's customized configuration file *Trident.cfg* on Volume 2

Using the PCMCIA/Floppy Switch

The PCMCIA/Floppy switch on the Flash System Controller board of an FN, LN, or CN determines where the router looks for the image and configuration file when booting. The PCMCIA (Personal Computer Memory Card International Association) position is for memory card boot access, and the Floppy position is for diskette boot access.

You can use Site Manager and the Technician Interface to access both the memory card and diskette files, regardless of the position of this switch. However, you cannot override the switch setting when booting. For example, you cannot boot from a diskette if the switch is set in the PCMCIA position.

When you use Site Manager to boot the router, or specify an image and configuration file in a Technician Interface **boot** command, the software verifies the file's existence before allowing the boot to take place.

If the PCMCIA/Floppy switch is in the PCMCIA setting, and you boot the router, the following occurs:

1. The router boots from **1:ace.out** if it is available. If not, it boots from **2:ace.out** if it is available. If both are unavailable, a boot error occurs.
2. The router configures from **1:config** if it is available. If not, it configures from **2:config** if it is available. If both are unavailable, a configuration error occurs.

Booting after Crossnet Shutdown Notification (BNX Only)

On BNX platforms only, you can use the **-shutdown** option of the **boot** command to boot the BNX following a "graceful crossnet shutdown." With this option, the system notifies the remote end of any configured Frame Relay Switch (frsw) PVCs to expect a loss of connectivity. (The BNX sends to the remote end of each PVC an update message packet with the A-bit set to"inactive.")

To initiate graceful shutdown followed by a system boot, enter the following command at the Technician Interface prompt:

boot -shutdown *<vol>*:*<image_name> <vol>*:*<config_name>*

The console displays the following message during shutdown:

```
Shutdown in progress.
```

If shutdown succeeds, the console displays the message

```
Shutdown is complete.
```

Upon issuing this message, the system performs a boot operation using the image and configuration files you specified originally.

If shutdown fails, the console displays the message

```
Continue shutdown? (Y/N)
```

If you choose "N" (no) at this time, the system terminates shutdown and displays the following message on the console device:

```
Shutdown aborted.
```

Upon issuing this message, the system performs a boot operation using the image and configuration files you specified originally.

If you choose instead to “Continue...?” (“Y”), the system continues the shutdown attempt. We recommend that you terminate this procedure after no more than one additional shutdown attempt.

Configuring Delayed Boot Services

You can configure the router to boot at a date and time that you specify. With Technician Interface commands, you

- Add delayed boot services to a router
- Schedule one or more nonrepeatable, delayed boot events on a router
- Name the router software image file and the router configuration file you want the router to use for a specific delayed boot event
- Manage (disable, re-enable, or delete) delayed boot services or specific delayed boot events configured on a router

The router’s RUIBOOT software supports all delayed boot services. Some Technician Interface commands you use to configure delayed boot services contain the RUIBOOT software entity name.

Adding Delayed Boot Services to a Router

Before scheduling any delayed boot events, you must add the RUIBOOT base record to the router configuration, as follows:

1. **Log in to the router’s Technician Interface.**

   Log in to the Technician Interface of the router you want to configure with a delayed boot event. If you need instructions on how to perform a login via local console or remote Telnet session, refer to Chapter 1.

2. **Define a slot mask for delayed boot services on the router.**

   Before creating the delayed boot service on the router, define a slot mask for the RUIBOOT entity. The slot mask identifies the slots on which the system will load and run RUIBOOT. At the Technician Interface prompt, enter

   ```
   BN [3]: set wfServices.wfRuiBootLoad.0 0x7FFE0000;commit
   ```

   This command allows RUIBOOT, once created, to run on all slots. The hexadecimal value **0x7FFE0000** works for any model of Bay Networks router, regardless of the number of slots in that router.

3. **Create a delayed boot service on the router.**

   Create the RUIBOOT service in the router configuration, as follows:

   ```
   BN [3]: set wfRuiBoot.wfRuiBootBaseDelete.0 1;commit
   ```

This also *enables* delayed boot services on the router. (The system sets the attribute wfRuiBootBaseDisable, OID = 1.3.6.1.4.1.18.3.3.2.14.1.1, in the RUIBOOT base record to its default value of 1 or enabled.)

Scheduling Delayed Boot Events

You can schedule a delayed boot event on a router as follows:

1. **Log in to the router's Technician Interface.**

Log in to the Technician Interface of the router you want to configure with a delayed boot event. If you need instructions on how to perform a login via local console or remote Telnet session, refer to Chapter 1, then resume the procedure for scheduling a delayed boot event.

2. **Schedule a delayed boot event.**

To schedule a delayed boot event, you must first create (add) an entry in the RUIBOOT table of delayed boot events, as follows:

```
BN [3]: set wfRuiBootTable.wfRuiBootDelete.<wfRuiBootDateAndTime>
1

BN [3]: commit
```

Note that the instance ID *<wfRuiBootDateAndTime>*

- Specifies when the delayed boot event will occur
- Comprises 11 octets, each of which contain in decimal notation one element of the date and time you want to specify for the boot event (see Figure 8-1)

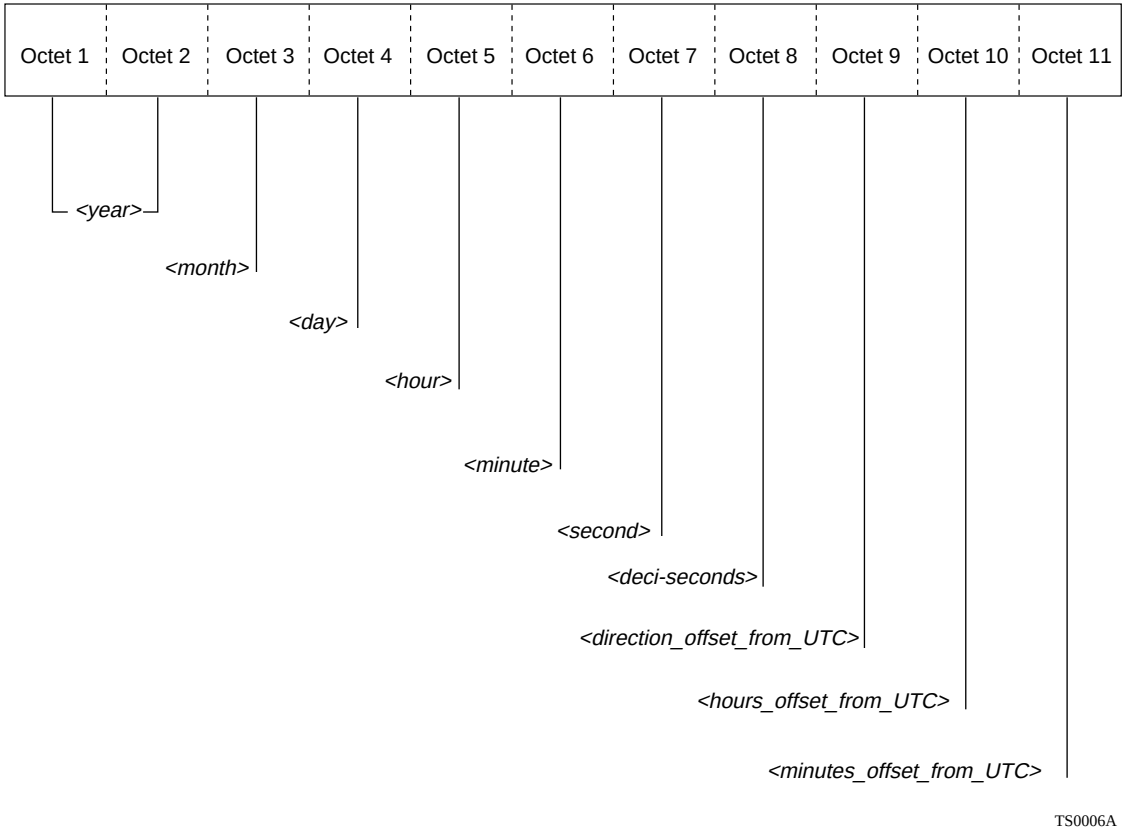


Figure 8-1. RUIBOOT Date and Time Entry

The following table specifies acceptable values for each octet of *<wfRuiBootDateAndTime>*:

Field	Allowable Values (in decimal notation)	Octet No.
Year	1996 to 9999	1 and 2
Month	1 to 12	3
Day	1 to 31	4
Hour	0 to 23	5
Minute	0 to 59	6
Second	0 to 60*	7
Deci-seconds	0 to 9	8
Direction offset from UTC	ASCII 43 (for “+”) ASCII 45 (for “-”)	9
Hours offset from UTC	0 to 11	10
Minutes offset from UTC	0 to 59	11
* Use 60 for leap-second.		

Example:

Schedule a delayed boot event for May 26, 1996, at 1:30:15 p.m., where the actual time and date at the location of the target router is offset from UTC (GMT) by -9 hours and 22 minutes.

Assuming that you have already enabled delayed boot services on the router, enter the following command line at the Technician Interface prompt:

```
set wfRuiBootEntry.wfRuiBootDateAndTime 19.96.05.26.13.30.15.00.45.09.22
```

Figure 8-2 shows how the values date, time, and UTC offset for this example map into the value of the 11-octet attribute, wfRuiBootDateAndTime.

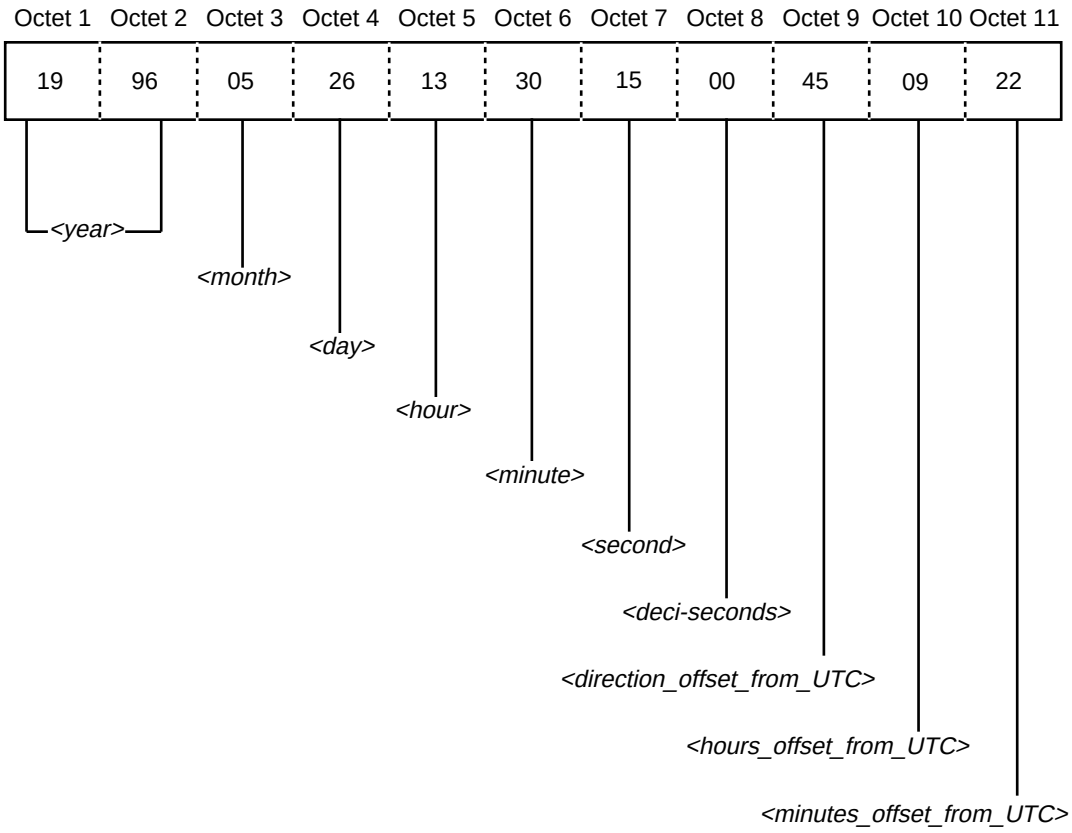


Figure 8-2. RUIBOOT Date and Time Example

3. Specify a boot image name.

Specify a router software image name for that entry, as follows:

`BN [3]:` **set wfRuiBootTable.wfRuiBootImageName.***<wfRuiBootDateAndTime>* **"bn.exe"**

`BN [3]:` **commit**

The name you specify belongs to the RUIBOOT table entry that has the same instance ID.

4. Specify a configuration file name, as follows:

```
BN [3]: set wfRuiBootTable.wfRuiBootConfigName.<wfRuiBootDateAndTime>
"config2"

BN [3]: commit
```

The name you specify belongs to the RUIBOOT table entry that has the same instance ID.

5. Schedule additional delayed boot events.

If you want to add more delayed boot events to the router configuration, return to step 2; otherwise, continue with step 6.

6. Save the current configuration file on the router, as follows:

```
BN [3]: save config <vol>:<filename>
```

Note: This is an optional step.

<*vol*> is the NVFS Flash volume on which you want to store a copy of the current (modified) configuration file on the router.

<*filename*> is the name you assign to the configuration file that contains your delayed boot entries.

7. Log out of the Technician Interface session.

```
BN [3]: logout
```

For more information on how to close a Technician Interface session with a Bay Networks router, refer to Chapter 1.

Managing Delayed Boot Services

This section describes how to

- Disable or re-enable delayed boot services on the router.
- Disable or re-enable a delayed boot event scheduled at an earlier time on the router.
- Change the name of the router software image and/or configuration file you want the router to boot with at a later time.
- Delete entries from the RUIBOOT table of delayed boot events.
- Delete delayed boot services from the router.

Disabling or Re-enabling Delayed Boot Services on a Router

You can, if necessary, disable the delayed boot service anytime after enabling it on a router. Enter the following command:

```
BN [3]: set wfRuiBoot.wfRuiBootBaseDisable.0 2;commit
```

Enter the following command to re-enable the delayed boot service after disabling it on a router:

```
BN [3]: set wfRuiBoot.wfRuiBootDisable.0 1;commit
```

Disabling or Re-enabling a Delayed Boot Event

Disable or re-enable a delayed boot event on the router, as follows:

1. **Enter the following command line to disable a delayed boot event anytime after adding it to the router configuration:**

   BN [3]: **set wfRuiBootEntry.wfRuiBootDisable.***<wfRuiBootDateAndTime>* **2;commit**

2. **Enter the following command line to re-enable a delayed boot event anytime after disabling it in the router configuration:**

   BN [3]: **set wfRuiBootEntry.wfRuiBootDisable.***<wfRuiBootDateAndTime>* **1;commit**

Modifying Attributes for Scheduled Delayed Boot Events

You can modify

- The name of the router software image file
- The name of the router configuration file

You cannot directly modify the date, time, or UTC offset (attribute wfRuiBootDateAndTime) for a scheduled boot event. If you need to change any of these for an existing entry in the RUIBOOT table of delayed boot events, proceed as follows:

- Delete the entry from the RUIBOOT table of delayed boot events
- Create a replacement entry

Deleting Delayed Boot Events

Delete a delayed boot event as follows:

```
BN [3]: set wfRuiBootEntry.wfRuiBootDelete.<wfRuiBootDateAndTime> 2;commit
```

You can save your change(s) to the current configuration file, as follows:

```
BN [3]: save config <vol>:<filename>
```

<*vol*> is the NVFS Flash volume on which you want to store a copy of the current (modified) configuration file on the router.

<*filename*> is the name you assign to the router's current configuration file.

Deleting Delayed Boot Services from the Router

If you want to delete delayed boot services from the router, change the setting for wfRuiBootDelete, a global parameter/attribute, as follows:

```
BN [3]: set wfRuiBoot.wfRuiBootBaseDelete.0  2;commit
```

Restarting a Slot

The **restart** command allows you to restart the GAME image currently in use on a specified slot or slots. Restarting a slot does not reboot with a new router software image. You restart a slot or slots by entering the slot number or numbers after the **restart** command. If you do not enter a slot number when issuing the **restart** command, all slots are restarted.

Enter the following to restart the entire system:

restart

Enter the **restart** command with one of the following parameters to restart a processor module or modules. <*slot_no.*> is the number of the slot where the processor module is located.

restart [<*slot_no.*>]

restart [<*slot_no.*>**-**<*slot_no.*>]

restart [<*slot_no.*>**,**<*slot_no.*>**,**. . .**,**]

Examples:

If you enter:	The system restarts:
restart	The entire system.
restart 1	Slot 1.
restart 1-5	Slots 1, 2, 3, 4, and 5.
restart 4,6	Slots 4 and 6.

Restarting After Crossnet Shutdown Notification (BNX Only)

On BNX platforms only, you can use the **-shutdown** option of the **restart** command to restart the GAME image on one or more slots, following a "graceful crossnet shutdown"on the same slots. With this option, the system notifies the remote end of any associated Frame Relay Switch (frsw) PVCs to expect a loss of connectivity. (The BNX sends to the remote end of each PVC an update message packet with the A-bit set to"inactive.")

To initiate graceful shutdown followed by a system or slot restart, enter the appropriate command at the Technician Interface prompt:

If you enter:	**The system performs a graceful shutdown and restarts**
restart -shutdown	All slots
restart -shutdown [*<slot_no.>*]	One slot
restart -shutdown [*<slot_no.>*-*<slot_no.>*]	A range of slots
restart -shutdown [*<slot_no.>*,*<slot_no.>*,. . . ,]	A list of slots

The console displays the following message during shutdown:

```
Shutdown in progress.
```

If shutdown succeeds, the console displays the message

```
Shutdown is complete.
```

Upon issuing this message, the system performs a restart operation.

If shutdown fails, the console displays the message

```
Continue shutdown? (Y/N)
```

If you choose "N" (no) at this time, the system terminates shutdown and displays the following message on the console device:

```
Shutdown aborted.
```

Upon issuing this message, the system performs a restart operation.

If you choose instead to “Continue...?” (“Y”), the system continues the shutdown attempt. We recommend that you terminate this procedure after no more than one additional shutdown attempt.

Resetting a System or Slot

The **reset** command allows you to reboot one or more slots with a new router software image. You reset one or more slots by entering the slot number or numbers after the **reset** command. If you do not enter a slot number when issuing the **reset** command, the entire system reboots with the default router software image and configuration. Entering the **reset** command without entering at least one slot number is equivalent to entering the **boot** command.

Enter the following to reset the entire system:

reset

The system returns the following message:

```
Reset all slots? (y/n)
```

If you still want to reset all slots, enter “y” (yes). Entering “n” (no) aborts the command.

Note: With multiple-slot routers (such as the BLN and BLN-2), a local Flash volume serves as a backup source for files required by any slot you want to reset. For this reason, multiple slot routers running Version 7.60 or later (with the dynamic loading feature) must contain a Flash volume that contains a copy of the router’s software image.

The following events occur when you reset a processor module:

1. The GAME operating system software running on the processor module forwards a boot request to the other processor modules.
2. The first processor module to respond to the boot request forwards the router software image resident in its memory.
3. The resetting processor module receives and executes the router software image. At this instant, connectivity to the associated slot and the services provided in the slot are disrupted. The other processor modules resynchronize their routing tables after the slot fails to receive packets.

4. The resetting processor module completes the boot process and requests a configuration. The first available processor module forwards the configuration resident in its memory.
5. The resetting processor module loads the configuration image and initiates the services provided by the slot; connectivity is thus reestablished. The resetting processor module alerts the other processor modules that it can receive packets.
6. The other processor modules resynchronize their routing tables accordingly.

To reboot the entire system, enter only **reset** at the command line prompt.

To reset only the processor module or modules you specify by *<slot_no.>*, enter the **reset** command as follows:

If you enter:	**The system resets:**
reset [*<slot_no.>*]	Reset one slot
reset [*<slot_no.>*-*<slot_no.>*]	Reset a range of slots
reset [*<slot_no.>*,*<slot_no.>*,. . . ,]	Reset a list of slots

Examples:

If you enter:	**The system reboots:**
reset	The entire system.
reset 1	Slot 1.
reset 1-5	Slots 1, 2, 3, 4, and 5.
reset 4, 6	Slots 4 and 6.

When you issue the **reset** or **reset slot** commands from a local console rather than from a Telnet session, the results depend on

- The slot number you designate in the command line
- The slot number from which you issue the command
- The model of Bay Networks router
- The type of router (single-slot or multislot)

Based on these variables, the router system or slot performs a restart, a warm-boot, or cold-boot operation. The following table describes the different responses.

	You issued a reset command from a Technician Interface session (console or Telnet) on one slot, and the target *<Slot_no.>* you specified was:		
	(None)	**The same slot the session is running on:**	**A slot other than the slot the session is running on:**
Command-> Router V	**reset**	**reset** *<Slot_no.>*	**reset** *<Slot_no.>*
AN ANH (single-slot routers)	Warm-boot Slot 1: • No diagnostics • Load new image on Slot 1 • Initialize new image on Slot 1 • Retain log info	Warm-boot Slot 1: • No diagnostics • Load new image on Slot 1 • Initialize new image on Slot 1 • Retain log info	N/A
AFN (single-slot router)	Warm-boot Slot 2: • No diagnostics • Load new image on Slot 2 • Initialize new image on Slot 2 • Retain log info	Restart Slot 2: • No diagnostics • No image reload on Slot 2 • Re-initialize current image on Slot 2 • Retain log info	N/A

	You issued a reset command from a Technician Interface session (console or Telnet) on one slot, and the target *<Slot_no.>* you specified was:		
	(None)	**The same slot the session is running on:**	**A slot other than the slot the session is running on:**
Command-> reset	**reset**	**reset** *<Slot_no.>*	**reset** *<Slot_no.>*
Router V			
ALN CN FN LN (multislot routers)	Warm-boot all slots: • No diagnostics • Load new image • Initialize new image • Retain log info on all Slots	Warm-boot the designated slot: • No diagnostics • Load new image on local slot • Initialize new image on local slot • Retain log info on designated slot	Cold-boot the designated slot: • Run diagnostics on the designated slot • Load new image on the designated slot • Initialize new image on the designated slot • Lose log info on the designated slot
BLN BLN-2 BCN (multislot routers)	Warm-boot all slots: • No diagnostics • Load new image • Initialize new image • Retain log info on all slots	Warm-boot the designated slot: • No diagnostics • Load new image on designated slot • Initialize new image on designated slot • Retain log info on designated slot	Warm-boot the designated slot: • No diagnostics • Load new image on the designated slot • Initialize new image on the designated slot • Retain log info on the designated slot

Note: If you reset the slot in which the Technician Interface is running, the Technician Interface resets with the next available slot on a multi-slot system, or with the same slot on a single-slot system.

Resetting After Crossnet Shutdown Notification (BNX Only)

On BNX platforms only, you can use the **-shutdown** option of the **reset** command to reset one or more slots, following a "graceful crossnet shutdown" on the same slots. With this option, the system notifies the remote end of any associated Frame Relay Switch PVCs to expect a loss of connectivity. (The BNX sends to the remote end of each PVC an update message packet with the A-bit set to"inactive.")

To initiate a graceful shutdown followed by a system or slot reset, enter the appropriate command at the Technician Interface prompt:

If you enter:	**The system performs a graceful shutdown and reset**
reset -shutdown	On all slots
reset -shutdown [*<slot_no.>*]	One one slot
reset -shutdown [*<slot_no.>-<slot_no.>*]	On a range of slots
reset -shutdown [*<slot_no.>*,*<slot_no.>*,. . . ,]	On a list of slots

The console displays the following message during shutdown:

```
Shutdown in progress.
```

If shutdown succeeds, the console displays the message

```
Shutdown is complete.
```

Upon issuing this message, the system performs the reset operation.

If shutdown fails, the console displays the message

```
Continue shutdown? (Y/N)
```

If you choose "N" (no) at this time, the system terminates shutdown and displays the following message on the console device:

```
Shutdown aborted.
```

Upon issuing this message, the system performs the reset operation.

If you choose instead to “Continue...?” (“Y”), the system continues the shutdown attempt. We recommend that you terminate this procedure after no more than one additional shutdown attempt.

Running Diagnostics

The **diags** command cold-starts one or more specified slots or the entire system. The cold start consists of CPU, backbone, and link diagnostics, and a reboot. If you do *not* enter a slot number, the system tests and reboots all slots.

Enter the following to run diagnostics on the entire system:

diags

The system returns the following message:

```
Perform diags on all slots? (y/n)
```

If you still want to run diagnostics on all slots, enter “y” (yes). Entering “n” (no) aborts the command.

Enter the **diags** command with one of the following parameters to run diagnostics and reboot one or more ILIs.

diags [*<slot_no.>*]

diags [*<slot_no.>*-*<slot_no.>*]

diags [*<slot_no.>*,*<slot_no.>*,. . . ,]

Examples:

If you enter:	The system:
diags	Runs diagnostics and reboots the entire system.
diags 1	Runs diagnostics for Slot 1 and reboots Slot 1.
diags 1-5	Runs diagnostics for Slots 1, 2, 3, 4, and 5 and reboots Slots 1, 2, 3, 4, and 5.
diags 4,6	Runs diagnostics for Slots 4 and 6, and reboots Slots 4 and 6.

The system runs diagnostics on the associated slot or slots, loads the router software image, loads the configuration, and initiates the router software services.

We recommend that you issue the **diags** command to the associated slot immediately after you hot-swap a board. Otherwise, the DIAG LED on the front panel and LED 8 on the FRE module remain on, indicating that diagnostics have *not* been run on the ILI. (Refer to the *Installing and Maintaining BN Routers* manual for more information.) If the board is functional, and you do *not* issue the **diags** command, the processor module automatically boots, loads the configuration, starts the router software services, and operates normally, although the DIAGS LED remains lit.

When you issue the **diags** or **diags** <*slot_no.*> commands from a local console rather than from a Telnet session, the results depend on

- The slot number you designate in the command line
- The slot number from which you issue the command
- The model of Bay Networks router
- The type of router (single-slot or multislot)

Based on these variables, the router system or slot performs a restart, a warm-boot, or a cold-boot operation. The following table describes the different responses:

	You issued a diag command from a Technician Interface session (console or Telnet) on one slot, and the target *<Slot_no.>* you specified was:		
	(None)	**The same slot the session is running on:**	**A slot other than the slot the session is running on**
Command->	**diag**	**diag** *<Slot_no.>*	**diag** *<Slot_no.>*
Router V			
AN ANH (single-slot routers)	Cold-boot Slot 1: • Run diagnostics on Slot 1 • Load new image on Slot 1 • Initialize new image on Slot 1 • Lose log info	Cold-boot Slot 1: • Run diagnostics on Slot 1 • Load new image on Slot 1 • Initialize new image on Slot 1 • Lose log info	N/A
AFN (single-slot router)	Warm-boot Slot 2: • No diagnostics • Load new image on Slot 2 • Initialize new image on Slot 2 • Retain log info	Restart Slot 2: • No diagnostics • No image reload • Re-initialize current image on Slot • Retain log info	N/A
ALN CN FN LN (multislot routers)	Cold-boot all slots: • Run diagnostics • Load new image • Initialize new image • Lose log info on all slots	Cold-boot the designated slot: • Run diagnostics on local slot • Load new image on local slot • Initialize new image on local slot • Lose log info on local slot	Cold-boot the designated slot: • Run diagnostics on the designated slot • Load new image on the designated slot • Initialize new image on the designated slot • Lose log info on the designated slot
BLN BLN-2 BCN (multislot routers)	Cold-boot all slots: • Run diagnostics • Load new image • Initialize new image • Lose log info on all slots	Cold-boot the designated slot: • Run diagnostics on designated slot • Load new image on designated slot • Initialize new image on designated slot • Lose log info on designated slot	Cold-boot the designated slot: • Run diagnostics on the designated slot • Load new image on the designated slot • Initialize new image on the designated slot • Lose log info on the designated slot

When you issue the Technician Interface **diags** command to test and reboot a specific module, the test and reboot process may take anywhere from 2 1/2 minutes to 10 minutes to complete, depending on the memory configuration of the board. For example, when you issue the **diags** command for a FRE-2 processor module with 8 MB of DRAM, the process takes approximately 3 minutes to complete. When you issue the **diags** command for a FRE-2 processor module with 32 MB of DRAM, the process takes approximately 10 minutes to complete.

Turning off the DIAG Indicator LED

The DIAG LED lights during diagnostics and goes out after diagnostics have determined that the processor module and its associated link module are functional. If they are not functional, the DIAG LED on the front panel and LED 8 on the FRE processor module daughterboard remain on. If this occurs, make sure the modules are seated properly in the router and issue the **diags** command again. Call your Bay Networks Technical Response Center if the DIAG LED does not go out.

If you hot-swap a Link Module, the diagnostics do not automatically run and the Fail LED on that module may remain ON. In this case, you can enter the following command to switch off the Fail LED:

diag -l *<slot_number>*

If you do not specify a slot number, the command switches off the Fail LED on all slots.

Displaying the Software Version

Enter **stamp** to display the current software version and the date and time it was created.

Halting Packet Transfer between Slots

When you reset a slot containing a processor (FRE or ACE) module, the router automatically halts packet transfer between the resetting slot and the other slots in the router. Packet transfer automatically resumes after the slot is operational again.

When you hot-swap a FRE module, the router also automatically halts and then resumes packet transfer.

When you hot-swap Bay Networks ACE module, be sure to enter the following Technician Interface command first, where <*slot_no.*> is the number of the slot containing the ACE you are going to hot-swap:

stop <*slot_no.*>

This command halts packet transfer between the slot you specify in the <*slot_no.*> field and the other slots in the router. When you insert another ACE module in the slot, ACE diagnostics automatically start up, the software resumes on the slot, and the other slots are informed that the slot in question is available for packet transfer.

Verifying and Upgrading Software

The Technician Interface provides the following commands for verifying and upgrading executable software:

- The **readexe** command calculates file header and image checksums on executable files on the file system, verifies that the checksums match those within the files, and displays the results and all file header information. Use this command to validate executable files before upgrading.
- The **prom -w** command erases the PROM and copies the contents of the PROM update file to the PROM. Use this command to update (write) a PROM with new software.
- The **prom -v** command compares the contents of a PROM file on the file system to the contents of a PROM. Use this command to verify that the software installed in the file system matches the software loaded on a PROM.

The executable software consists of the following binary files:

- *frediag.exe* is the diagnostics image file. To upgrade with a new diagnostics image, transfer the new *frediag.exe* file to the file system, issue the **readexe** command to validate it, and issue the **prom -w** command to load (write) it onto the diagnostics PROM. The diagnostics PROM device supplies the FRE processor module with diagnostic instructions during a cold start.

  If you want to verify that the image resident on the diagnostics PROM matches the *frediag.exe* file, use the **prom -v** command.

- *freboot.exe* is the bootstrap image file. To upgrade with a new bootstrap image, transfer the new *freboot.exe* file to the file system, issue the **readexe** command to validate it, and issue the **prom -w** command to load (write) it onto the bootstrap PROM. The bootstrap PROM supplies the FRE module with bootstrap instructions during a cold start.

  If you want to verify that the image resident on the bootstrap PROM matches the *freboot.exe* file, use the **prom -v** command.

- *bn.exe* is the router software image for the BLN, BLN-2, and BCN. *an.exe* is the router software image for the AN and ANH. *afn.exe* is the router software image for the AFN. *asn.exe* is the router software image for the ASN. *ace.out* is the router software image for the FN, LN, CN, and ALN. When the system boots, it automatically loads the default router software image (unless you specify another router software image) from another slot into memory on the processor module or, if another slot is unavailable, from the file system to memory. To upgrade with a new image, transfer it to the file system and reset the system; do *not* use the **prom -w** command when upgrading with a new router software image.

Note: You cannot edit executable files.

The sections that follow describe how to use the **readexe**, **prom -w**, and **prom -v** commands to validate, upgrade, and verify executable software.

Validating an Executable File

You validate executable files before upgrading by using the **readexe** command. This command calculates file header and image checksums on executable files on the file system, verifies that the checksums match those within the files, and displays the results and all file header information.

Enter the following command and parameter to validate an executable file on the active volume. <*filename*> is the name of the executable file.

readexe *<filename>*

Enter the following command and parameters to validate an executable file on another volume:

readexe *<vol>*:*<filename>*

<*vol*> is the volume storing the file.

<*filename*> is the name of the executable file.

Figure 8-3 shows a sample system response to the **readexe** command.

```
$ readexe 5:bn.exe
Processing contents of '5:bn.exe'...

---------------------------------
-- Module name:   krnl_bn.exe
---------------------------------
   Validating header checksum... OK
   Validating image checksum...  OK

   Program execution address space:
   --------------------------------
   Load Address: 0x30300000  Size: 767449 Bytes  Entry point:  0x00000000

   PROM storage address space:
   ---------------------------
   PROM Load address: 0x00000000

   Input file information:
   -----------------------
   Platform Key: (0101000B) BB M68000 MotherBoard (FRE FRE2 FRE2_60)
   Workspace:    int/8.10/40
   Compression:  ON
   Revision:     8.10
   Last Modifed: Friday December 30 18:44:14 1994
   File type:    Executable file
   Tool name:    Oasys Linker
```

Figure 8-3. Sample Response to readexe Command

The system response to the **readexe** command contains the following information:

- Validating header checksum. The system calculates a checksum on the file's header and compares the checksum to the data in the checksum field of the file's header. The system reports that the header checksum is *OK* if it matches or *BAD* if it does not match.
- Validating image checksum. The system calculates a checksum on the file's image data and compares the checksum to the data in the checksum field of the image. The system reports that the image checksum is *OK* if it matches or *BAD* if it does not match.

- `Program execution address space` provides information about where the file is located in memory.
  - -- `Load Address` indicates the memory location.
  - -- `Size` indicates the size of the file.
  - -- `Entry point` indicates the location in memory of the first software instruction when the file is loaded into memory. This field is 0 if the file is compressed.
- `PROM storage address space` indicates the location in the PROM for the *frediag.exe* and *freboot.exe* software. This field is 0 if the file is not stored in a PROM.
- `Input file information` contains the following information about the file:
  - -- `Platform Key` indicates the platform that the file is intended to run on.
  - -- `Workspace` indicates the software release and software integration numbers.
  - -- `Compression` indicates whether the file is compressed. The executable files are normally compressed.
  - -- `Revision` indicates the software release.
  - -- `Last Modified` indicates day, date, and time of the software release.
  - -- `File type` indicates that the file is executable.
  - -- `Tool name` is for Bay Networks use only.

Examples:

If you enter:	The system:
readexe frediag.exe	Calculates file header and image checksums on the *frediag.exe* file located on the active volume, verifies that the header and image checksums match those within the file, and displays the results and all file header information.
readexe 3:freboot.exe	Calculates file header and image checksums on the *freboot.exe* file located on Volume 3, verifies that the header and image checksums match those within the file, and displays the results and all file header information.

Upgrading and Verifying a PROM

You use the **prom** command to upgrade or verify the software on a diagnostics or bootstrap PROM in a Bay Networks router or BNX platform. Only users who login as "Manager" can access the **prom** command.

Caution: If a software release includes a PROM software upgrade, see the upgrade documentation shipped with the software for instructions on upgrading the PROMs on your router. The instructions describe

- How to determine the models of router that need a PROM update
- How to determine whether you must upgrade the PROM(s) in a specific model of router by using the Technician Interface prom command, or by physically replacing the existing PROM device with a new PROM device
- How the PROM upgrade process works
- How to determine the current versions of PROM images residing in a router
- What you need to know about upgrading PROMs in a remote router
- How to specify the commands necessary to upgrade and verify a PROM

- If you do not follow these instructions, you may disable the router you are trying to upgrade.

During an update, the system erases the image stored in the target PROM and writes the new image into the PROM. This is sometimes called “burning” the PROM. To verify the image update, the system compares the contents of the new image file to the image file in the PROM.

Upgrading PROMs Remotely

Because the operations involved in upgrading PROMs place an increased load on the router, there is a greater chance that the PROM upgrade process will time out or fail during periods of peak traffic on your network.

Caution: If the PROM upgrade process is interrupted, the router could be disabled.

Follow these guidelines to ensure that the PROM upgrade is successful:

- Store the PROM executable files (for example, *frediag.exe* or *freboot.exe*) on a Flash card that resides on the least utilized slot in the system.
- Perform the upgrade during non-peak hours to ensure a minimum traffic load on the router.
- On multislot systems, upgrade the PROM for each slot separately. Attempting to upgrade multiple slots at the same time increases the load on the backplane.

Determining Current PROM Image Versions

To decide whether or not you need to upgrade the PROMs in a router, you need to determine the versions of Boot and Diagnostics PROM images currently running in that router.

Note: A label on the back panel of some router models indicates the installed version of Boot and Diagnostic PROMs.

Determining the Version of the Current Boot PROM Image

To determine the version number of Boot PROM images residing in a router, start a Telnet session with the router and enter the following command at the Technician Interface prompt:

get wfHwEntry.19.*

With a Model BLN router, for example, information similar to the following appears, with one `wfHwEntry.wfHwBootPromSource` line for each slot.

```
wfHwEntry.wfHwBootPromSource.1 = (nil)

wfHwEntry.wfHwBootPromSource.2 = "rel/8.10/freboot.exe"

wfHwEntry.wfHwBootPromSource.3 = "rel/8.10/freboot.exe"

wfHwEntry.wfHwBootPromSource.4 = "rel/8.10/freboot.exe"

wfHwEntry.wfHwBootPromSource.5 = "rel/8.10/freboot.exe"
```

Each line of response to the command specifies

- A slot number (for example, "`wfHwEntry.wfHwBootPromSource.`**`2`**" identifies Slot 2).
- A pathname that contains the version number of the image stored in the Boot PROM (for example, "`rel/8.10/freboot.exe`" identifies the Version 8.10 Boot PROM image *freboot.exe* in Slot 2).

Note: The command does not return a Boot PROM version number for slot 1 because slot 1 contains a System Resource Module (SRM). This applies to all models of router except AN and ASN routers.

Determining the Version of the Current Diagnostics PROM Image

To determine the version number of DIAG PROM images residing in a router, start a Telnet session with the router and enter the following command at the Technician Interface prompt:

get wfHwEntry.16.*

With a Model BLN router, for example, information similar to the following appears, with one `wfHwEntry.wfHwDiagPromSource` line for each slot:

```
wfHwEntry.wfHwDiagPromSource.2 =
"/harpdiag.rel/v4.00/wf.pj/harpoon.ss/image.p/frediag.exe"

wfHwEntry.wfHwDiagPromSource.3 =
"/harpdiag.rel/v4.00/wf.pj/harpoon.ss/image.p/frediag.exe"

wfHwEntry.wfHwDiagPromSource.4 =
"/harpdiag.rel/v4.00/wf.pj/harpoon.ss/image.p/frediag.exe"

wfHwEntry.wfHwDiagPromSource.5 =
"/harpdiag.rel/v4.00/wf.pj/harpoon.ss/image.p/frediag.exe"
```

Each line of response to the command specifies

- A slot number (for example, "`wfHwEntry.wfHwDiagPromSource.`**`2`**" identifies Slot 2).
- A pathname that contains the version number of the image stored in a diagnostics PROM (for example, `"/harpdiag.rel/v4.00/wf.pj/harpoon.ss/image.p/frediag.exe"` identifies the "v4.00" (Version 4.0) diagnostics PROM image *frediag.exe* in Slot 2).

Using the prom Command

Note: Before upgrading any router software, always save a copy of the original configuration file and boot image as a safeguard, in case you encounter problems during the procedure.

To upgrade the PROMs:

1. **Insert a Flash card with contiguous free space sufficient to accommodate the PROM images you want to use as source files for upgrading boot or diagnostic PROMs on one or more slots.**

   To determine the amount of contiguous free space, display the directory of the Flash volume by entering the following command from the Technician Interface prompt:

   dir <*volume_no.*>**:**

If you need more contiguous free space for the image:

- Delete unnecessary or obsolete files.
- Compact the contents of the Flash card.

2. **Transfer the PROM image files (for example,** *freboot.exe* **and** *frediag.exe***) to the Flash card.**

   From the Technician Interface, use the **tftp** command. (Refer to "In-Band File Transfers" in Chapter 4 if you need more information.)

3. **Establish a Technician Interface session with the router.**

   Refer to Chapter 1 if you need more information on how to open a Technician Interface session with the router.

4. **If you are updating a Boot PROM, enter**

   prom -w *<volume_no.>*:*<Boot_PROM_source_file> <slot_ID >*

   For example:

   prom -w 2:freboot.exe 3

Note: Once you enter the **prom** command**,** it must run to completion. The control-c (abort) command is disabled for the duration of the **prom** command execution to allow it to run to completion. Upgrading takes from 2 to 10 minutes per PROM. Verifying takes up to 2 minutes per PROM.

5. **If you are updating a Diagnostic PROM, enter**

   prom -w *<volume_no.> <Diag_PROM_source_file> <slot_ID >*

   For example, to upgrade the diagnostics PROMs in Slots 2 through 5, you can enter

   prom -w 2:frediag.exe 2-5

Caution: When upgrading PROMs with new software, upgrade all slots that contain FRE modules to avoid a mismatch of software.

More examples of command lines appear at the end of this section.

6. **To verify successful completion of a PROM upgrade, enter**

   prom -v *<volume_no.> <Diag_PROM_source_file> <slot_ID >*

   For example, for a boot PROM, enter

   prom -v *<volume_no.>***: [freboot.exe** | **asnboot.exe** | **anboot.exe]** *<slot_ID>*

   For a diagnostics PROM, enter

   prom -v *<volume_no.>***: [frediag.exe** | **asndiag.exe** | **andiag.exe]** *<slot_ID>*

   The system verifies that the PROM image on a designated Flash volume (that is, the image file used as a source for upgrading the PROM) matches the image actually stored in the boot or diagnostics PROM on a designated slot.

   When you use the **-v** option, the console displays one of the following messages after the verification routine terminates:

   ```
   prom: slot <slot_ID> completed successfully
   ```

   ```
   prom: PROM data does not match file data on slot <slot ID>
   ```

   If the operation succeeds, the new images stored in the boot and diagnostics PROMs run when you reboot the router.

   If the operation fails, the console displays a message describing the cause of the failure.

Additional Examples:

If you enter:	The system:
prom -v 2:frediag.exe 3	Verifies the contents of the diagnostics PROM on Slot 3 against the contents of the *frediag.exe* file on Volume 2.
prom -w 2:freboot.exe 3	Erases the bootstrap PROM on Slot 3 and copies the contents of the *freboot.exe* file on Volume 2 to the PROM on Slot 3.
Any one of the following: **prom -w 2:frediag.exe 2, 3, 4, 5** **prom -w 2:frediag.exe 2 3 4 5** **prom -w 2:frediag.exe 2, 3-5** **prom -w 2:frediag.exe 2-5**	Erases the diagnostics PROMs on Slots 2, 3, 4, and 5 and copies the contents of the *frediag.exe* file on Volume 2 to the PROMs on Slots 2, 3, 4, and 5.

Viewing the Load Addresses and Sizes of Applications

The **loadmap** command allows you to view the load address and size of each dynamically loadable application.

Enter the **loadmap** command with one or more of the following optional parameters to view the addresses and sizes of the applications located on a specified slot or slots. <*slot_no.*> is the number of the slot where the applications are located (you can also enter the keyword **all** to view the applications for all slots). <*filename*> is the name of the file to which you want to direct the output.

loadmap [<*slot_no.*>] [<*filename*>]

loadmap [<*slot_no.*>-<*slot_no.*>] [<*filename*>]

loadmap [<*slot_no.*>,<*slot_no.*>,. . .] [<*filename*>]

If you enter the **loadmap** command without entering a slot number, the system dumps the addresses and sizes of all applications on all slots to the specified filename. If you do not specify a destination filename, the system displays the addresses and sizes of the applications on the screen.

Examples:

If you enter:	**The system:**
loadmap	Displays the load addresses and sizes for all applications on all slots on the screen.
loadmap 3 4 5	Displays the load addresses and sizes for all applications on Slots 3, 4, and 5 on the screen.
loadmap 3-8	Displays the load addresses and sizes for all applications on Slots 3, 4, 5, 6, 7, and 8 on the screen.
loadmap all 2:map.dump or **loadmap 2:map.dump**	Dumps the load addresses and sizes for all applications on all slots to the specified file.

The following example shows a sample screen display when you issue the **loadmap** command without any optional parameters. (If no applications reside on a slot, the message `No dynamically loadable modules on SLOT #` appears.)

```
No dynamically loadable modules on SLOT 4
----------------------
Loadmap from SLOT 2:
----------------------
--> vines.exe        0x304a5c60  0118168
--> drs.exe          0x30467550  0060288
--> tms380.exe       0x304760e0  0089652
--> hdlc.exe         0x304caaf0  0055608
--> dst.exe          0x30526400  0004052
----------------------
Loadmap from SLOT 5:
----------------------
--> fr.exe           0x310b9f00  0026760
--> hdlc.exe         0x310c67d0  0055608
--> qsync.exe        0x3111c630  0004008
----------------------
Loadmap from SLOT 3:
----------------------
--> arp.exe          0x3048c0d0  0008816
--> ipx.exe          0x303fec60  0087680
--> at.exe           0x303e4e90  0105916
--> vines.exe        0x30448f20  0118168
--> ftp.exe          0x30418310  0042060
--> tcp.exe          0x30422770  0057040
--> tftp.exe         0x304b9c90  0020680
--> snmp.exe         0x30430650  0030344
--> tn.exe           0x304bed70  0038424
--> ip.exe           0x3048e350  0178468
--> ilacc.exe        0x304cb670  0011872
--> qenet.exe        0x30523f10  0004072
```

Setting the ACE Backplane Type

The **backplane** command allows you to set or display the ACE backplane type in nonvolatile RAM. You issue the **backplane** command during the initial startup of your VME-based Bay Networks router. You need only enter the **backplane** command once during the life of the system controller installed in Slot 1 of the router, unless you insert the system controller in another type of VME router. For instructions on using the **backplane** command, see *Quick-Starting Routers and BNX Platforms*.

Enter the following command to set the ACE backplane type in nonvolatile RAM. <*type*> is the VME-based router type (ALN, LN, CN, or FN).

backplane <*type*>

If you issue the **backplane** command without specifying a type, the system displays the router's backplane type to the screen.

Examples:

If you enter:	The system:
backplane	Reads the backplane type from the hardware and displays the type to the screen.
backplane LN	Sets the backplane type to LN. Use for LN or ALN.
backplane CN	Sets the backplane type to CN.
backplane FN	Sets the backplane type to FN.

Resetting the Date and Time

The **date** command allows you to display or change the system date, time, or time zone offset. The time is based on the 24-hour clock. The offset is the time difference between the current time and Greenwich Mean Time (GMT).

Enter the following to display the system date, time, and GMT offset:

date

The date, time, and GMT offset are displayed in *mm/dd/yy hh:mm:ss +|- hh:mm* format. For example:

```
Jan 16, 1995 15:26:23 [GMT+12]
```

The GMT offset is stored as a direction (+ or -) and a value in hours and minutes. Most time zone offset values are in hours, and do not include minutes. For example, the eastern standard time (EST) zone is 5 hours behind GMT (or GMT-5).

Enter the following to change the date, time, and GMT offset:

date [*<mm/dd/yy hh:mm:ss>* [**+**|- *hh:mm*]]

The console displays the new date, time, and time zone offset.

If you do not enter a parameter (for example, the date), the system uses the current system setting.

Note: When you change the date, time, and GMT offset, the GAME operating system distributes the new date and time to all processor modules.

Changing the GMT offset changes the timestamps of messages in the event log. For example, the GMT offset was 0 at 2:00 p.m. At 10:00 p.m., you access the event log to check the messages that came in between 2:00 and 10:00. If you then change the GMT offset to -2, the timestamp of each message in the event log is offset by -2 hours (that is, if the timestamp was 2:00 p.m., it changes to 12:00 p.m.).

Examples:

If you enter:	The following occurs:
date	The console displays the current system date, time, and time zone offset: `Jan 25, 1995 16:00 [GMT-4]`
date 01/25/95 16:02	The system date and time change to: `Jan 25, 1995 16:02`
date 01/25/95 16:02 -5	The system date, time, and time zone offset change to: `Jan 25, 1995 16:02 [GMT-5]`

Assigning Passwords

This section describes how to assign or reassign the Manager and User access passwords.

The Technician Interface runs on a single processor module. When you assign a password, the GAME operating system distributes the new password to nonvolatile RAM in all processor modules. (For this reason, the system retains passwords if the Technician Interface runs subsequently on a different processor module, after you booted the router, reset a slot, or replaced a board.)

Note: If you insert a new processor module, you must reassign the Manager and User passwords; otherwise, the Technician Interface will not require passwords when it runs on that slot.

You can assign the User access password when you are logged in as User or Manager. You can assign the Manager access password only when you are logged in as Manager.

Note: Passwords, as well as Technician Interface commands and filenames, are case sensitive.

Proceed as follows to assign a password:

1. **Enter the following to display or assign a password:**

   password [**Manager** | **User**]

   The console displays one of the following messages:

   ```
   Changing password for User
   ```

   ```
   Changing password for Manager
   ```

2. **Proceed to Step 3 if you are logged in as Manager and you are changing the User password. Otherwise, enter the old password at the following prompt:**

   ```
   Old password:
   ```

   If there is no old password, press the return key.

3. **Enter the new password after the following prompt:**

   ```
   New Password:
   ```

   The password may have 0 to 16 alphanumeric characters. If you want to remove password protection, press the return key.

4. **Repeat Step 3 after the following prompt:**

   ```
   Retype new password
   ```

   The console displays one of the following messages:

   ```
   User password changed
   ```

   ```
   Manager password changed
   ```

   If you enter the wrong password, the console displays the following message:

   ```
   User password not changed
   ```

   The $ prompt reappears.

   If you do not reply to password prompts within about 30 seconds, the system cancels the **password** command and displays the following messages:

   ```
   ** Input timed out. **
   ```

   ```
   Command aborted
   ```

   The $ prompt reappears.

Enabling and Disabling SecurID Authentication

This section describes how to enable or disable SecureID services from a Technician Interface session.

Note: You enable/disable SecureID services only from a router console (an ASCII terminal or terminal emulator connected directly to the router console port). You cannot enable/disable SecureID services through a Technician Interface session supported by means of Telnet connection to the router.

To enable or disable SecureID services, you answer questions from the *securelogin* configuration utility running on the router. Press Return after each entry. If you press Return without entering a response to a question, *securelogin* repeats the last question.

Enabling SecurID Authentication

Once you log in to the Technician Interface and the $ prompt appears on the console display, proceed as follows to enable SecureID authentication services on the router:

1. **Enter the following at the Technician Interface prompt:**

   $: securelogin

2. **Respond to each question that appears on your console display. (The sequence shows responses as bold text within brackets.)**

   ```
   Do you wish telnet login to require SecurID? (yes/no) [yes]
   ```

   ```
   What is the IP address of the router being secured? (a.b.c.d)
   [<IP_Address>]
   ```

   ```
   What is the IP address of the SecurID server? (a.b.c.d)
   [<IP_Address>]
   ```

   ```
   What is the TCP port number for SecurID services? (default=755)
   [<TCP_Port_Number>]
   ```

   ```
   You have designated <IP_Decimal_Address>
   (<IP_Hexadecimal_Address>) as your SecurID server.
   ```

   If you accepted the default port, the following message appears on your console display:

   ```
   The default port 755 will be used for SecurID services.
   ```

If you entered a different port number, the following message appears on your console or Telnet display:

```
The port <port_number> will be used for SecurID services.
Is this information correct? (yes/no) [yes]
```

3. **If you entered *no*, go to step 4; otherwise, *securelogin* replies with**

   ```
   Telnet login now requires SecurID.
   ```

   followed by

   ```
   Reinitialize Client? (yes/no) [yes]
   ```

   a. **If you entered *no*, go to step 3b; otherwise, *securelogin* replies with**

   ```
   Client reinitialized.
   ```

   You have completed the procedure. The SecureID client software on the router has been reinitialized. If you want to disable SecureID login for Telnet users, follow the procedure in the next section, “Disabling SecureID Authentication.”

   b. **If you entered *no*,** *securelogin* **replies with**

   ```
   Client not reinitialized.
   ```

   You have completed the procedure, but the SecureID client software on the router has not been reinitialized.

4. **You entered *no*, indicating that the information about SecurID setup was incorrect.**

   ***securelogin* replies with:**

   ```
   Do you still wish telnet login to require SecurID? (yes/no) [yes]
   ```

   If you entered *yes*, return to step 2; if you entered *no*, go to step 5.

5. **You entered *no*, indicating that you do not want Telnet users to encounter the SecureID login procedure. *securelogin* replies with**

   ```
   Securelogin information remains unchanged
   Are you sure you want to turn off secure ID? (yes/no) [yes]
   ```

   If you entered *yes*, *securelogin* replies with

   ```
   SecurID no longer required on Telnet login!
   ```

   You have completed the procedure, and you have not changed any configuration information for the SecureID client software on the router.

Disabling SecureID Authentication

Once the Technician Interface login prompt appears ($, or whatever your network administrator has set up for a prompt), proceed as follows to disable SecureID authentication services already enabled and active on the router:

1. **Run the *securelogin* configuration utility.**

   ```
   $: securelogin
   ```

2. **Respond to each of the questions that appear in your Telnet or console display. Press Return after each entry, beginning with**

   ```
   Do you wish to secure telnet login? (yes/no) [yes]
   ```

   Entering *yes* invokes an additional verification.

   ```
   Are you sure you want to turn off secure ID? (yes/no) [yes]
   ```

   If you entered *yes*, *securelogin* replies with

   ```
   SecurID no longer required on Telnet login!
   ```

   If you entered *no*, *securelogin* replies with

   ```
   Secure login information remains unchanged!
   ```

   If you entered *no* and received the reply `Secure login information remains unchanged!`, the SecureID client is still enabled on the router. Telnet users continue to encounter the SecureID login procedure before acquiring access to the router's Technician Interface.

Managing SNMP Secure Mode

Bay Networks implements an optional security mechanism for all SNMP **set** requests. This proprietary mechanism is an interim solution to solve some of SNMP's security problems until a stable, widely accepted industry-standard security solution is available.

Our security system uses counters to synchronize management operations between manager and agent. In secure mode, when Site Manager sends a **set** request to the router, the request includes the encrypted value of a counter plus 1 as the first variable binding in the PDU.

When the agent on the router receives the **set** request, it compares the decrypted value with the value of its own counter plus 1. If the two values match, the agent considers the **set** request to be authentic and increments the counter by 2. The agent stores the new value of the counter in an encrypted form in the MIB and sends it back to Site Manager as the first variable binding in the response.

The manager receiving the response validates that the received counter matches the manager's counter plus 2. If the two values match, the response is declared authentic.

The use of counters guards against masquerade security violations because an intruder would have to know the encryption key and the correct counter to send as the first variable binding. The security mechanism also guards against message stream modification; an intruder cannot reorder a sequence of **set** requests because the requests' counters would not match the next sequence expected by the agent.

The following sections describe the Technician Interface commands you use to manage the security feature.

Setting the Router to Operate in Secure Mode

The **wfsnmpmode** command allows you to specify whether or not you want the router to operate in snmp secure mode.

Enter the **wfsnmpmode** command in the following format:

wfsnmpmode [**1** | **3**]

1 (trivial) indicates that the router should provide no additional security beyond a simple community name.

3 (proprietary) indicates that the router should operate using our proprietary security mechanism.

Note: Do not use the default (Public) community and wildcard manager (0.0.0.0) with the router in snmp secure mode. Instead, configure a specific SNMP community and manager address. For more information on how to configure SNMP communities, refer to *Configuring SNMP, BOOTP, DHCP, and RARP Services*.

Setting the Encryption Key

Use the **wfsnmpkey** command to specify the key that the encryption algorithm uses when it encrypts the security counters. The encryption algorithm uses the attributes of the key (size, range, and value) as integral parts of its encryption process.

Also, when Site Manager issues the first **set** request within an application, it prompts the user to enter this key as a password that enables Site Manager to operate in secure mode.

Enter the command in the following format:

wfsnmpkey *<key>*

<key> is the string of ACSII characters that make up the encryption key for this router. The key can be no longer than six characters.

Note: If you replace a board in a BCN, BLN, or BLN-2 router, you should re-enter the **wfsnmpkey** command to ensure that the key is updated for all slots.

Resetting the Security Counter

The **wfsnmpseed** command allows you to reset the counter used by the security mechanism. Under normal operating conditions, it is not necessary to reset the counter; this command is mainly for debugging purposes.

To reset the seed counter, enter the **wfsnmpseed** command in the following format:

wfsnmpseed *<comm_name> <mgr_address>* [**-**|*<value>*] [**-**|*<value>*] [**-**|*<value>*] [**-**|*<value>*] [**-**|*<value>*]

<comm_name> is the name of the SNMP community for which you want to reset the counter.

<mgr_address> is the address of the manager for which you want to reset the counter.

[**-**|*<value>*] is either a dash (-) to indicate no change to a specific counter value, or the value to which you want to reset the counter.

Example:

If you enter:	The manager with address 192.32.1.20 in community “public”:
wfsnmpseed public 192.32.1.20 - 23 - 44 -	Sets the second counter to 23 and the fourth counter to 44. The first, third, and fifth counters are not changed.

Customizing Hardware Compression Search Depth

If you have model BLN, BLN-2, and BCN routers configured to run frame relay on circuits of an Octal Sync link module, you can customize the depth of search for tokens to replace data patterns sent and received by the optional Octal Sync Hardware Compression daughterboard.

Note: For more information on hardware and software compression services, refer to the *Configuring Data Compression Services* guide.

By increasing the search depth, you may enable the daughterboard to attain compression ratios higher than are possible using default or inherited search depth values. (The results you achieve depend greatly on the type of data you want to compress over a circuit or line.) Note, however, that increasing the compression ratio beyond a certain value on a circuit or line may also lower the throughput on that circuit or line. Configure search depth attributes for the best trade-off between compression ratio and end-to-end (for example, workstation-to-workstation) throughput on the circuit or line.

Use Technician Interface commands to customize

- wfWcpLineSearchDepth
- wfWcpCircuitSearchDepth

Note: Only expert network technicians or administrators should attempt to modify the set value of these WCP attributes. You cannot modify these attributes from a Site Manager workstation.

Testing Compression and Throughput

Perform the following tests before and after making any change to the set values of the line and circuit WCP search depth attributes:

- Measure end-to-end throughput for several file transfer operations across the circuit(s) or line for which you are changing the search depth value. Select files that contain data representative of the type of information your organization needs to send and receive daily.
- Measure the percentage of bandwidth utilization required to send your test file(s) over the synchronous line.
- Calculate the compression ratio(s) resulting from the file transfer operations

Compare your compression ratios and line utilization figures taken before and after your changes. Determine from these results whether you have improved the configuration for data compression on the desired line and/or circuit(s).

The best settings for the search depth attributes result in the best trade-offs between end-to-end throughput, compression ratios, and line costs for the type of data you want to send over a synchronous line.

WCP Search Depth Attributes

The modifiable search depth attributes for the WCP entity have the following characteristics:

Parameter:	**WCP Line Search Depth**
Attribute Name:	wfWcpLineSearchDepth
Attribute Number:	9
Default:	3
Options:	0 (no compression on this line) to 255 (maximum compression on this line)
Function:	Defines the depth of searching for repetitive patterns in the data you want to send over a synchronous *line*. Unless you also configure search depth at the *circuit* level independently (using wfWcpCircuitSearchDepth), any virtual circuit you configure on this line inherits the setting for line search depth.
Instructions:	Compression ratios may improve with settings higher than the default value of 3; however, throughput may actually decrease for settings higher than 12 or 13. (The compression engine yields higher compression ratios, but takes longer to find token matches for the data being sent over the line.) Bay Networks does not recommend settings higher than 13. Accept the default value or choose a customized search depth value that provides the best trade-off between compression ratio and throughput on this line. Test end-to-end throughput and line utilization before and after modifying the WCP search depth attributes.
Command:	**set wfWcpLineEntry.wfWcpLineSearchDepth** *<0 - 255>*
MIB Object ID:	1.3.6.1.4.1.18.3.4.22.1.1.9

Parameter:	**WCP Circuit Search Depth**
Attribute Name:	wfWcpCircuitSearchDepth
Attribute Number:	7
Default:	256
Options:	0 (no compression on this circuit) to 255 (maximum compression on this circuit), or 256 (inherit wfWcpLineSearchDepth value on this circuit)
Function:	Defines the depth of searching for repetitive patterns in the data you want to send over a specific (virtual) circuit. Whenever you choose a customized value (within the range 0 to 255) for wfWcpCircuitSearchDepth, you automatically choose not to inherit the wfWcpLineSearchDepth value.
Instructions:	Compression ratios may improve with settings higher than 3 (the value inherited from the wfWcpLineSearchDepth attribute); however, throughput may actually decrease for settings higher than 12 or 13. (The compression engine yields higher compression ratios, but takes longer to find token matches for the data being sent over the circuit.) Bay Networks does not recommend settings higher than 13. Accept the default value to inherit the wfWcpLineSearchDepth value on this circuit, or choose a customized value that provides the best trade-off between compression ratio and throughput on this circuit. Test end-to-end throughput on this circuit before and after modifying the WCP circuit search depth value.
Command:	**set wfWcpCircuitEntry.wfWcpCircuitSearchDepth** *<0 - 255 | 256>*
MIB Object ID:	1.3.6.1.4.1.18.3.4.22.2.1.7

Displaying a Greeting or Notice Before the Login Prompt

You can create a greeting, notice, caution, or warning message that displays before the Technician Interface `Login:` prompt. To create and initialize this message on the router, proceed as follows:

1. **Create an ASCII file named *ti_notice.txt* on your UNIX workstation or PC.**
2. **Enter the text of a greeting or notice message that meets your requirements.**

   Format the message with appropriate spacing and return characters.

Note: The router software imposes no limit on the size of the message (in kB). However, the file system volume (Flash card) where the *ti_notice.txt* file resides must have contiguous free space sufficient to accommodate your message. Depending on the setup of a user's console device or Telnet application, the topmost lines of a long pre-login message may scroll out of view. For this reason, we recommend that you limit the length of your message to less than 20 lines.

3. **Save *ti_notice.txt* on your workstation or PC.**
4. **Use TFTP to copy *ti_msg.txt* to the router's default file system volume.**

Whenever someone attempts to log in to the router, the message appears on the router's local console display or the remote user's Telnet screen.

Customizing the Technician Interface Welcome Message

You can modify or replace the login message `Welcome to the <router_model> Technician Interface` according to the needs of your organization or network site. The Technician Interface software invokes the message from an ASCII text file named *ti_msg.txt*.

To replace or customize the Welcome message on a particular router:

1. **Back up or copy *ti_msg.txt* to another filename (such as *ti_msg.txt.orig*) on the router.**

   You may want to restore the default Welcome message at some later time.

2. **Use TFTP to copy *ti_msg.txt* from the router to your UNIX workstation or PC.**

3. **Open *ti_msg.txt* on your workstation or PC.**

4. **Edit the default Welcome message, or enter a replacement message up to 256 characters in length.**

   Format the message with appropriate spacing and return characters.

5. **Save your new version of *ti_msg.txt*.**

6. **Use TFTP to copy *ti_msg.txt* back to the router.**

   The new version of the file replaces the original version on the router.

Recording Console Messages to a File

Use the **record** command to record to a file all messages the system sends to the console terminal. In this way, you can save the output of Technician Interface commands and, if necessary, forward the results to Bay Networks customer support personnel.

Open the record file before recording, then close the file when you finish recording. You can lose the file if it is not closed before you unmount the file system or reset the router.

Enter the following command to open the record file and record messages to that file:

record open [**-fileonly**] [**-pause**] *<vol>:<filename>*

open creates and opens a record file. The system sends command output and messages to both the console terminal and the file.

[**-fileonly**] writes messages only to the file, not to the terminal. Use this option only within a script. (This option allows a script to write to a file.) By default, the system writes messages to both the terminal and the file.

[**-pause**] immediately places the system in pause mode. Use this option with the **-fileonly** option.

<*vol*> is the slot number containing the volume used to store the file.

<*filename*> is the name of the file used to store the output.

You can suspend recording temporarily by using the **pause** option.

You can determine the state of recording by testing the global variable RECORD_STATE from a script. ON indicates the system is recording, OFF indicates recording is turned off, and PAUSED indicates that recording is temporarily suspended. To display the pause state of the record command, enter the following:

record pause

To change the pause state, enter

record pause [**on** | **off**]

on disables recording.

off re-enables recording.

To close the record file and save it, enter the following command:

record close

Note: When you specify a record file on a Flash (NVFS) volume, remember that only one record file at a time can be open on that volume. If you attempt to concurrently write other Technician Interface commands to another open record file on the same volume, those commands will fail.

Enabling Internal Clocking Mode

Within test environments and when using the HSSI Crossover Cable (Order No. 7832), you may need to configure Bay Networks routers from the Technician Interface to enable internal clocking mode. Enter the following at the Technician Interface prompt:

set wfHssiEntry.wfHssiInternalClkTestMode.4.1 1;commit

The default value, 2, enables external clocking. The new value, 1, enables internal clocking.

Enter the following to display the new value:

get wfHssiEntry.wfHssiInternalClkTestMode.4.1

The Technician Interface displays

```
wfHssiEntry.wfHssiInternalClkTestMode.4.1 = 1
```

Be sure to enter the following to set the variable back to external clocking to use the external clock source:

set wfHssiEntry.wfHssiInternalClkTestMode.4.1 2;commit

Responding to QENET Underflow Errors

Transmit underflow errors can occur when a QENET link module is connected to a FRE module and all four ports are transmitting. This often occurs when non-SNAP encapsulated frames received from an FDDI ring are routed out the interface of a QENET. An example of such a frame is a Novell proprietary encapsulated frame on FDDI.

The wfCSMACDUfloTx attribute in the wfCSMACDEntry MIB object shows the number of transmit underflow errors. These errors result in other stations detecting CRC errors.

Enter the following Technician Interface command for each of the four connectors only if you are experiencing transmit underflow errors as described above:

set wfCSMACDEntry.wfCSMACDAlignmentMode.<*slot no.*>.<*connector*>
1;commit

Then save the configuration with these changes to the configuration file.

When you set the wfCSMACDAlignmentMode attribute to 1 (ALIGN_ALL), the router realigns the nonoptimally aligned frames before transmitting them.

When you set the wfCSMACDAlignmentMode attribute to 3 (DISABLED), the router transmits the nonoptimally aligned frames without realigning them first.

When you set the wfCSMACDAlignmentMode attribute to 2 (ALIGN_OVER_128_BYTES), the router realigns the nonoptimally aligned frames exceeding 128 bytes before transmitting them, and transmits the nonoptimally aligned frames of 128 bytes or less without realigning them first.

Monitoring ip Routes

The **ip** command allows you to display IP data from any of the following sources:

- The main routing table for any slot
- The internal cache for any slot
- The routing cache for a specific logical interface
- The multicast routes cache
- The BGP routes table for any BGP peer
- The OSPF Link State Data Base (LSDB)

You choose the source by specifying a <*subcommand*> in the command line. You can also selectively filter the data by specifying one or more option <*flags*> in the command line.

Enter the **ip** command as follows:

ip <*subcommand*> <*flags*>

<*subcommand*> = <**routes**| **bgp_routes** | **cache** | **ospf_lsdb**>

The subcommands have the following meanings:

If you enter the subcommand:	The system displays
routes	The routing table you select by specifying appropriate command flags. RIP and EGP routes refresh only on slots that receive route updates. Route ages may be different on each slot for this reason.
bgp_routes	The BGP routing table you select by specifying appropriate command flags. Lists routes announced to various configured BGP peers.
cache	The routing cache you select by specifying appropriate command flags. The cache subcommand requires an interface address. For unnumbered interfaces, use 0.0.0.0 with the circuit option.
ospf_lsdb	The contents of the ospf_lsdb you select by specifying appropriate command flags.

<flags> = [*<IP_address>* | *<IP_address/prefix>* | **-a***<area_address>* | **-A** | **-c***<circuit_no.>* | **-i** *<BGP_router_ID>* | **-M** | **-N** | **-p** [*<local_peer_address* | *remote peer address>*] | **-S***<source_address>* | **-s***<slot_number>* | **-t***<type_number>*]

The *<flags>* apply to subcommands, as follows:

Flag	Filtering Effect	Applicable Subcommand(s)
<address>	Retrieves data for IP addresses that match your address entry in dotted decimal notation	routes | bgp_routes | cache | ospf_lsdb
<address/prefix>	Retrieves data for IP addresses with an address mask that matches your entry. Specify an IP address in dotted decimal notation. Specify the number of bits in the address mask by entering a decimal number (1 to 24, starting with the msb) in the */prefix* portion of your entry.	routes | bgp_routes | ospf_lsdb |
-a *<area_address>*	Retrieves data for the OSPF area you specify after the **-a** flag.	ospf_lsdb
-A	Retrieves • The entire table of routes, including best routes and routes not used or: • The entire OSPF LSDB (20 lines max. per route advertisement)	routes | ospf_lsdb
-c *<circuit_no.>*	Retrieves data for the circuit number you specify after the **-c** flag. (See “Determining Circuit Numbers” later in this chapter.)	cache
-i *<BGP_router_ID>*	Retrieves routes to or from a BGP peer that you specify after the **-i** flag.	bgp_routes
-M	Retrieves only the contents of the multicast cache	cache
-N	Retrieves the BGP ANNOUNCE table of routes.	bgp_routes
-p [*<local_peer_address | remote_peer_address>*]	Retrieves routes announced to a BGP peer you specify by its local or remote address.	
-S *<source_address>*	Retrieves data pertaining only to the advertising source you specify after the **-S** flag.	ospf_lsdb

-s *<slot_number>*	Retrieves data for the slot you specify after the -**s** flag. If you also specify an address of 255.255.255.255 for a given slot, the command displays only the internal cache for that slot. If you do not enter a slot number, the command retrieves only data pertaining to the slot where the Technician Interface is running.	routes | bgp_routes | cache
-t *<type_number>*	Retrieves data for the OSPF LS type (type of Link State advertisement) that you specify after the **-t** flag, as follows: 0 = stub advertisement 1 = router links advertisement 2 = network links advertisement 3 = summary link (IP network) advertisement 4 = summary link (ASBR) advertisement 5 = external link advertisement For more information on LS Types, refer to RFC 1583.	ospf_lsdb

Example (ip routes)

Enter the following command to display the table of IP “best” (used or active) routes:

ip routes

```
Network/Mask      Proto  Age    Slot   Cost   NextHop Address   AS
----------------- ------ ------  -----  ------  ----------------  --
2.0.0.0/8         RIP    30     2      5      192.168.125.33
10.0.0.0/8        RIP    30     2      3      192.168.125.33
122.0.0.0/8       RIP    30     2      5      192.168.125.33
131.192.0.0/16    RIP    30     2      3      192.168.125.33
132.245.0.0/16    RIP    30     2      3      192.168.125.33
134.177.0.0/16    RIP    30     2      3      192.168.125.33
140.200.0.0/16    RIP    30     2      3      192.168.125.33
162.78.0.0/16     RIP    30     2      3      192.168.125.33
.
.
.

Total Networks on Slot 2 = 268
```

Data from the **ip routes** command excludes inactive or unused routes that exist in the complete table of IP routes. To view the complete table, including inactive/unused routes, use the **ip routes -A** command.

Example (IP routes)

Enter the following command to display the entire table of routes, including inactive/unused and best routes:

ip routes -A

```
 Network/Mask        Proto      Age  Sl   Cost  NextHop Address /   AS  Weight
 ------------------ ------ -------- -- -------- ----------------/----- --------
*0.0.0.0/0          RIP          20  2        2 192.32.174.33          7b9e0002
 0.0.0.0/0          Direct      385  0   131071 Unreachable            ffffffff
 0.0.0.0/32         Host        N/A  0        0 un# IP cct 0           00000000
*6.0.0.0/8          Direct      385  2        0 6.6.6.6                00000000
 6.0.0.0/32         Host        N/A  2        0 Broadcast              00000000
 6.6.6.6/32         Host        N/A  2        0 This Router            00000000
 6.255.255.255/32   Host        N/A  2        0 Broadcast              00000000
*128.128.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*129.128.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*130.128.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*131.119.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*134.177.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*141.251.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*146.240.0.0/16     RIP          20  2        2 192.32.174.33          7b9e0002
*170.41.0.0/16      RIP          20  2        2 192.32.174.33          7b9e0002
*172.14.0.0/16      RIP          20  2        2 192.32.174.33          7b9e0002
*172.15.0.0/16      RIP          20  2        2 192.32.174.33          7b9e0002
*192.1.1.0/24       RIP          20  2        2 192.32.174.33          7b9e0002
*192.1.2.0/24       RIP          20  2        2 192.32.174.33          7b9e0002
*192.32.1.0/24      RIP          20  2        2 192.32.174.33          7b9e0002

   Total Networks on Slot 2 = 268
```

The asterisk indicates best routes, or routes currently being used by IP.

Example (bgp routes)

Enter the following command to display the entire BGP table of routes:

ip bgp_routes

```
Network/Mask   Peer Rem Addr    NextHop Address  Org  Loc Pref  Best/Used
-------------- ---------------- ---------------- --- ---------- ---------
4.0.0.0/8       3.3.3.2          3.3.3.2          IGP   8183    BEST/USED
     As Path: SEQ 200
5.0.0.0/8       2.2.2.3          2.2.2.3          IGP   8183
     As Path: SEQ 300
...
SLOT 2: Total Nets 2
SLOT 5: Total Nets 7
```

When you specify the **-i**, **-p**, or **ip_address** options for the **ip bgp_routes** command, the resulting display specifies the total number of networks, plus the following additional information:

- *Multi-exit-disc (Multiple-exit discriminator)* -- RFC1771 defines this as an optional, nontransitive attribute that is a four-octet, nonnegative integer. A BGP speaker uses the value of this attribute to help discriminate among multiple exits to a neighboring autonomous system (AS).
- *Aggregator* -- RFC1771 defines this as an optional transitive attribute of length 6. The attribute contains the last AS number that formed the aggregate route (encoded as 2 octets), followed by the IP address of the BGP speaker that formed the aggregate route (encoded as 4 octets).

Example (bgp routes)

Enter the following command to display routes announced to the peer with a local address of 3.3.3.1 and a remote address of 3.3.3.2.

ip bgp_routes -N -p3.3.3.1/3.3.3.2

```
Network/Mask       Peer Rem Addr    NextHop Address  Org  Loc Pref
------------------ ---------------- ---------------- --- ----------
1.0.0.0/8          3.3.3.2          3.3.3.1          IGP         -1
     As Path: SEQ 100
     Multi-exit-disc -1  Aggregator 100 192.32.140.40
2.0.0.0/8          3.3.3.2          3.3.3.1          IGP         -1
     As Path: SEQ 100
     Multi-exit-disc -1
...
SLOT 5: Total Peers 1 Total Nets 256
   256 Routes To 3.3.3.1/3.3.3.2                 IGP:5 EGP:0 INC:251.
```

For **ip bgp_routes -N**, the display specifies

- Total number of peers
- Total number of networks
- Total number of routes announced to the first 5 peers on each slot

Example (bgp routes)

Enter the following command to display routes announced to BGP peers known to the local router:

ip bgp_routes -N

```
Network/Mask        Peer Rem Addr  NextHop Address Org  Loc Pref
------------------ -------------- -------------- --- ----------
192.32.174.4/30    192.32.175.130  192.32.175.129  IGP
   As Path: SEQ 2
192.32.174.8/30    192.32.175.130  192.32.175.129  IGP
   As Path: SEQ 2
192.32.174.32/27   192.32.175.130  192.32.175.129  IGP
   As Path: SEQ 2
192.32.174.96/27   192.32.175.130  192.32.175.129  IGP
   As Path: SEQ 2
192.32.174.128/27  192.32.175.130  192.32.175.129  IGP
   As Path: SEQ 2
192.32.174.160/27  192.32.175.130  192.32.175.129  INC
   As Path: SEQ 2
192.32.174.192/27  192.32.175.130  192.32.175.129  INC
   As Path: SEQ 2

SLOT 4: Total Peers 1 Total Nets 7
      7 Routes To 192.32.175.129/192.32.175.130    IGP:5 EGP:0 INC:2.
```

Example (ospf_lsdb)

Define a command to display the OSPF Link State Database for Type 1 link states in area 0.0.0.0.

ip ospf_lsdb -t1 -a0.0.0.0

The following is a typical response from the router:

```
LS Type Link State ID  Adv Router  Metric  ASE Fwd Addr Age  Seq Nbr
------- -------------  ----------  ------  ------------  ---  ---------
Router  192.32.174.62  192.32.174.62  100              1904 80000009
Router  192.32.174.65  192.32.174.65    1              1773 8000000b
Router  192.32.174.66  192.32.174.66    1              1707 8000000c
```

The column headings in screens invoked by the **ip** command have the following meanings:

* (asterisk)	Indicates routes actively used by IP, versus routes not currently used. (The asterisk appears only when you specify the all routes [**-A**] flag.)
Adv Router	Indicates the OSPF Router ID of the advertisement's originator. For router links advertisements, this field is identical to the Link State ID field. The network's Designated Router originates Network Link advertisements. Area border routers originate Summary Link advertisements. AS boundary routers originate AS External Link advertisements.
Age	Number of seconds since this route was last updated or verified to be correct. The meaning of "too old" depends on the routing protocol specified under Proto. Note that RIP and EGP routes are refreshed only on a slot that receives a routes update. Route ages may be different on each slot for this reason.
ASE Fwd Addr	An address for forwarding packets to a destination external to the AS, but not accessible through an AS boundary router.
Cost	Number of hops to reach the destination.
Link State ID (LSID)	Indicates the piece of the routing domain that the advertisement describes, as follows: If LS Type = 1, LSID = the originating router's Router ID. If LS Type = 2, LSID = the IP interface address of the network's Designated Router If LS Type = 3, LSID = the destination network's IP address. If LS Type = 4, LSID = the Router ID of the AS boundary router. If LS Type = 5 , LSID = the destination network's IP address.
Loc Pref	A discretionary attribute used by a BGP speaker to inform other BGP speakers in its own autonomous system of the originating speaker's degree of preference for an advertised route.
LS Type	Indicates the type of OSPF Link State advertisement, as follows: 0 = stub advertisement 1 = router links advertisement 2 = network links advertisement 3 = summary link (IP network) advertisement 4 = summary link (ASBR) advertisement 5 = external link advertisement Refer to RFC 1583 for more information on LS Type.

Mask	Subnet mask to be combined with the destination address and then compared with the value in Destination. If the value of Destination is 0.0.0.0 (a default route), then the mask is 0.0.0.0 (Prefix = 0).
Metric	Indicates the costs of the various interfaces described in a router LS Type advertisement. Also indicates the cost of each path described in summary link and AS external link advertisements.
Network	Destination IP address for this route, where 0.0.0.0 indicates a default route.
NextHopAddr / AS	IP address of the next hop and next Autonomous System of this route. If the next hop is an unnumbered interface, the command displays `un# IP cct <n>`, where *n* is the number of the circuit on which the interface has been configured.
Org	Origin of the path information (EGP, IGP, or INCOMPLETE).
Peer Rem Addr	The remote address of a BGP peer.
Proto	Routing method through which the router learned this route: Other, Local, Netmgmt, ICMP, EGP, BGP, Hello, RIP, IS-IS, OSPF, or BGP.
Seq Nbr	A signed 32-bit integer used to detect old and duplicate link-state advertisements. The larger the sequence number (when compared as signed 32-bit integers) the more recent the advertisement.
Sl (or) Slot	Number of the slot on which the network address/mask is configured.
Weight	Weight value assigned to the route (displayed only if you specify all routes [**-A**].

Routing Tables

Each *slot* on the router maintains an independent routing table (or “routing pool”). The table is the default (but not initial) source for a slot to look up routing information necessary to forward locally received packets.

Each routing table continuously receives, from IP and all other nonmulticast IP protocols configured on the router, updates on routes added, changed, or deleted in your network. By means of this continuous, high-speed, internal update mechanism, the system synchronizes the contents of routing tables on all slots. (The only exceptions to this rule occur during the first 10 seconds of a router boot or slot reset operation.)

Unlike the **show ip** script command, which retrieves from the router's active MIB an aggregated view of data from IP routing tables and internal caches across all slots, the Technician Interface **ip** command retrieves the contents of the routing table on a single slot that you specify. For this reason, the **ip** command retrieves information significantly faster than the **show ip** command.

With the **ip** command, you can examine

- The entire contents of the routing table on any slot
- A subset of the total contents of the routing table on any slot

You limit the view of a routing table by applying filters -- subcommand options and flags -- to the **ip** command syntax. For example, you can enter **ip routes** -*<s>*, where -*<s>* is a slot number you specify.

Note: RIP and EGP routes are refreshed only on a slot that receives a routes update. Route ages may be different on each slot for this reason.

Interface Cache

The router operating system allocates a cache storage space to each protocol-specific *logical interface* that you define on any physical circuit of the router. The interface cache stores routing information relevant only to itself and its own view of the networks external to the router.

This cache provides an initial source for an interface to retrieve at high speed the best routes to any other IP destination address in your network. Upon receiving a packet, the interface checks its local cache, then specifies processing for the packet:

- Encaps processing -- The packet will be forwarded out of the interface.
- Reassembly processing -- The packet is for this router.
- Redirect processing -- An ICMP Redirect packet will be sent from the interface, back to the source.
- Net Unreachable processing -- An ICMP Net Unreachable packet will be sent from the interface, back to the source.
- Host Unreachable processing -- An ICMP Host Unreachable packet will be sent from the interface, back to the source.

- ARP processing -- The packet has been held and an ARP request packet has been sent to the LAN for that host. When the address is resolved, the cache entry for this host is flushed (deleted) and the packet is forwarded.
- Multicast processing -- The packet will be handled using information from the multicast cache. (More information follows on the multicast cache.)

The internal cache is limited in size, and operates on a first-in, first-out (FIFO) basis. For this reason, cache entries (routes) also have a finite lifetime dictated largely by the size (depth) of the internal cache. (The larger the size of the internal cache, the longer it takes for an entry in that cache to expire.)

With the **ip** command, you can examine the entire contents of the cache for a specific logical interface configured on the router. To view the cache for any interface configured on the router, enter the **ip** command using the following syntax:

ip cache *<interface_address>*

<interface_address> is the IP address of the logical interface associated with the interface cache you want to examine.

Multicast Cache

If you enable a multicast protocol on a circuit, the system allocates and maintains one multicast cache for that circuit. Each entry in a multicast cache entry identifies the hosts (sources) and multicast groups from which the local circuit is receiving multicast traffic.

With the **ip** command, you can examine the entire contents of the multicast cache for a specific physical circuit. To view the multicast cache for any circuit configured on the router, enter the **ip** command using the following syntax:

ip cache -M *<interface_address>*

<interface_address> is the IP address of the logical interface associated with the multicast cache you want to examine.

Slot/Internal Cache

The router operating system maintains an “internal” cache storage space on (and for) each slot in the router. This slot-level, internal cache stores routing information captured from traffic originated on the router. For example, the PING protocol, the IP protocols, and TFTP can each generate their own traffic destined for IP address locations internal or external to the router.

The internal cache provides to such protocols a local, high-speed database of best routes from that slot to any other IP destination address in your network.

If the protocol application cannot find in the internal cache a route to the desired destination, then it searches the main routing table to find one. Once the application finds a route in the main routing table, it adds that route to the internal cache for the local slot.

If the routing table changes (with old routes replaced by new routes), the changes also propagate to the internal cache on the same slot.

The internal cache is limited and fixed in size, and operates on a first-in, first-out (FIFO) basis. For this reason, cache entries (routes) also have a finite lifetime determined by the size (depth) of the internal cache. (The larger the size of the internal cache, the longer it takes for an entry in that cache to disappear.)

With the **ip** command, you can examine

- The entire contents of the internal cache on any slot
- A subset of the total contents of the cache on any slot

To view the internal cache on any slot, enter the **ip** command using the following syntax:

ip cache 255.255.255.255 *-<s>*

-<s> is a slot number.

255.255.255.255 is the default address bit mask for the internal cache on any slot.

OSPF Link State Database

With the **ip** command, you can examine

- The entire contents of the router's OSPF Link State Data Base (OSPF LSDB)
- A subset of the detailed contents of the router's OSPF LSDB

To view the OSPF LSDB, enter the **ip** command using the following syntax:

ip cache ospf_lsdb -<A | a> -s -t

-A invokes the complete OSPF LSDB, for all OSPF areas known to the router (20 lines maximum per advertisement).

-a is the address of the OSPF area associated with the LSDB you want to view.

-s is the slot number associated with the LSDB you want to view.

-t is the OSPF LS Type indicator (stub, router, network, summary link, or external).

Determining Circuit Numbers

Whenever you create a new circuit via the Technician Interface or the Configuration Manager tool, the router operating system software (GAME) maps the circuit *name* you assign (such as "E21") to a circuit *number* (such as "4") in the router's active MIB.

When you use the Technician Interface **ip** command to display data pertaining only to a specific circuit on a router, you must enter the circuit number after the **-c** option flag for that command.

Example:

The following **ip** command displays all IP routes accessible via circuit 4 on the router. (The command shows the contents of the cache for an unnumbered IP interface on circuit 4.)

ip cache 0.0.0.0 -c4

You can determine the circuit number from the router's active MIB by using the Technician Interface **get** command in a variety of ways.

Example:

The following command retrieves the circuit number (attribute 6) for every entry in the FDDI Line_Table:

$ g wfFddiEntry.6.*

```
wfFddiEntry.wfFDDICct.5.1 = 1
```

(The table has a single line entry.)

Example:

The following command retrieves the circuit number (attribute 6) for every entry in the CSMACD Line_Table:

$ g wfCSMACDEntry.6.*

```
wfCSMACDEntry.wfCSMACDCct.2.1 = 3

wfCSMACDEntry.wfCSMACDCct.2.3 = 2
```

Example:

The following command retrieves the circuit number (attribute 5) for every entry in the IP Interface table:

$ g wfIpInterfaceEntry.5.*

```
wfIpInterfaceEntry.wfIpInterfaceCircuit.192.32.174.33.3 = 3

wfIpInterfaceEntry.wfIpInterfaceCircuit.192.32.174.66.4 = 4

wfIpInterfaceEntry.wfIpInterfaceCircuit.192.32.174.98.2 = 2

wfIpInterfaceEntry.wfIpInterfaceCircuit.192.32.175.66.1 = 1
```

The instance ID for each entry in this case is <*IP_address.circuit_number*>:

Example:

The following command retrieves the circuit number (attribute 2) for every entry in the Circuit Name table:

$ g wfCircuitNameEntry.2.*

```
wfCircuitNameEntry.wfCircuitNumber.1 = 1
wfCircuitNameEntry.wfCircuitNumber.2 = 2
wfCircuitNameEntry.wfCircuitNumber.3 = 3
wfCircuitNameEntry.wfCircuitNumber.4 = 4
```

Technician Interface Commands and Access Levels

The Technician Interface provides two access levels:

- User access level accepts read-only commands.
- Manager access level accepts all Technician Interface commands.

Table 8-4 lists all Technician Interface commands and their associated access levels.

Table 8-4. Technician Interface Access Levels

Command	User	Manager
!	✔	✔
alias	✔	✔
arrayenv (refer to *Writing Technician Interface Scripts*)	✔	✔
atmarp	✔	✔
attr (DOS only)	✔	✔
backplane		✔
bconfig		✔
boot		✔
cd	✔	✔
clearlog		✔

Table 8-4. Technician Interface Access Levels *(continued)*

Command	User	Manager
commit		✔
compact (NVFS only)		✔
copy		✔
cutenv (refer to *Writing Technician Interface Scripts*)	✔	✔
date	✔	✔
delete		✔
diags		✔
dinfo (NVFS only)	✔	✔
dir	✔	✔
disable (refer to *Using Technician Interface Scripts*)		✔
echo (refer to *Writing Technician Interface Scripts*)	✔	✔
enable (refer to *Using Technician Interface Scripts*)		✔
enumenv (refer to *Writing Technician Interface Scripts*)	✔	✔
exec		✔
export (refer to *Writing Technician Interface Scripts*)	✔	✔
format (NVFS only)		✔
get	✔	✔
getenv (refer to *Writing Technician Interface Scripts*)	✔	✔
gosub (refer to *Writing Technician Interface Scripts*)	✔	✔
goto (refer to *Writing Technician Interface Scripts*)	✔	✔
help	✔	✔
history	✔	✔
if (refer to *Writing Technician Interface Scripts*)	✔	✔
ifconfig		✔
instenv (refer to *Writing Technician Interface Scripts*)	✔	✔
ip	✔	✔
label (DOS only)		✔

Table 8-4. Technician Interface Access Levels *(continued)*

Command	User	Manager
let (refer to *Writing Technician Interface Scripts*)	✔	✔
list	✔	✔
loadmap		✔
log	✔	✔
logout	✔	✔
mibget (refer to *Writing Technician Interface Scripts*)	✔	✔
mkdir (DOS only)		✔
more	✔	✔
mount (DOS only)	✔	✔
octetfmt (refer to *Writing Technician Interface Scripts*)	✔	✔
on	✔	✔
osidata	✔	✔
partition	✔	✔
password Manager		✔
password User	✔	✔
pause (refer to *Writing Technician Interface Scripts*)	✔	✔
ping	✔	✔
pktdump (refer to *Troubleshooting Routers*)		✔
printf (refer to *Writing Technician Interface Scripts*)	✔	✔
prom		✔
readexe	✔	✔
record		✔
rename (DOS only)		✔
reset		✔
restart		✔
return (refer to *Writing Technician Interface Scripts*)	✔	✔
rmdir (DOS only)		✔

Table 8-4. Technician Interface Access Levels *(continued)*

Command	User	Manager
run (refer to *Writing Technician Interface Scripts*)	✔	✔
save aliases		✔
save config		✔
save env (refer to *Writing Technician Interface Scripts*)		✔
save log		✔
set		✔
setenv (refer to *Writing Technician Interface Scripts*)	✔	✔
show (refer to *Using Technician Interface Scripts*)	✔	✔
source aliases	✔	✔
source env (refer to *Writing Technician Interface Scripts*)	✔	✔
sprintf (refer to *Writing Technician Interface Scripts*)	✔	✔
stamp	✔	✔
stop (LN and CN only)		✔
string		✔
system	✔	✔
telnet	✔	✔
tftp		✔
type	✔	✔
unalias	✔	✔
unmount (DOS only)	✔	✔
unsetenv (refer to *Writing Technician Interface Scripts*)	✔	✔
verbose	✔	✔
wfsnmpkey		✔
wfsnmpmode		✔
wfsnmpseed		✔
xmodem		✔

Chapter 9
Managing Aliases

An alias is a command you create to take the place of long or multiple commands. After creating the alias, you enter the alias name to invoke its associated commands.

This chapter describes how to do the following:

- Create an alias in memory and enter its name to invoke its associated commands
- Display the commands associated with an alias
- Debug an alias
- Delete an alias
- Save aliases to a file in the NVFS for later retrieval
- Load aliases from a file into RAM
- Use the aliases in the *debug.al* file to debug common network problems

Creating and Displaying an Alias

You can use the **alias** command either to create an alias or to display the commands associated with an existing alias. Enter the following to display or create an alias:

alias [*<name>* [[**"**]*<alias_value>*[**"**]]]

<name> is one of the following optional alias name types:

- The name of the alias you are creating. The name may be one to 15 alphanumeric characters; the initial character must be alphabetical.
- The name of an existing alias, when you want to display its associated commands.

<alias_value> is a string of Technician Interface commands. The following rules apply to inserting characters in the *<alias_value>*:

- Separate commands with a space and a semicolon (;).
- Use double quotes (“ ”) *outside* the *<alias_value>* if it includes a space or a semicolon (;). The quotes are otherwise optional.
- Enter a backslash (\) before every quote character *inside* the *<alias_value>*. This includes the quotes in an **echo** command embedded within the *<alias_value>*.
- Enter a backslash (\) before the following characters when you use them literally: another backslash (\), a percentage sign (%), or a dollar sign ($) at the last character position of the *<alias_value>*.
- Limit the *<alias_value>* to 255 bytes of data (just over three 80-character lines).

You can create an alias that invokes other aliases by entering the **alias** command and nesting up to 15 other aliases in the *<alias_value>* argument. Separate the aliases with a space and a semicolon (;). (Refer to the last example in the examples that follow.)

When you create an alias, the system stores it in memory. Use the **save** command (described in a later section) to save the aliases in RAM to a file for later retrieval. The system can store up to 100 aliases in memory, provided that memory isn’t dedicated to other tasks, so limit the number of aliases in an alias file to 100. You can store as many alias files in your file system as space allows.

Examples:

If you enter:	The system:
alias	Displays all aliases residing in RAM.
alias ebridge “set wfBrTp.2.0 1; set wfBrStp.2.0 1;commit”	Creates an alias named *ebridge* that invokes the listed commands.
ebridge	• Enables the Translating Bridge and the Spanning Tree Bridge. • Notifies all relevant software modules of set changes to the MIB.
alias gbridge “get wfBrTp.2.0; get wfBrStp.2.0”	Creates an alias named *gbridge* that **gets** the Translating Bridge and Spanning Tree Bridge Enable values.
alias sbridge “ebridge;gbridge”	Creates an alias named *sbridge* that invokes the aliases *ebridge* and *gbridge*.

Inserting Parameters in an Alias

You can insert one or more parameters in an <*alias_value*> when creating an alias. You can insert a parameter in an <*alias_value*> in two ways:

- *Parameter concatenation*: You can insert a dollar sign (**$**) in the last character position of the <*alias_value*>. Then, when a user enters the alias name and follows it with the value of the parameter, the system executes the alias with the value the user entered.
- *Parameter reference:* You can embed one or more parameters anywhere inside the <*alias_value*>. For each parameter you embed when creating the alias, you insert a percentage sign (**%**) and a parameter number. The parameter **%1** in an <*alias_value*> takes the value of the first parameter the user enters at the command line after the alias name; the parameter **%2** in an <*alias_value*> takes the value of the second parameter the user enters, and so on.

Note: You cannot combine the two methods of inserting parameters within an alias.

The parameter number indicates the position of the value in the user entry. This feature allows you to use the same value for more than one parameter. (Refer to the last two examples.)

Examples:

If you enter:	The system:
alias scroll "more $"	Creates an alias named *scroll* that invokes the **more** command and inserts the value the user enters when using the alias (as shown in the next example).
scroll on	Invokes the command **more on**.
alias cp "copy 2:%1 3:%2"	Creates an alias named *cp* that accepts two values and inserts them in parameter positions **%1** and **%2**, respectively (as shown in the next example).
cp config2.cfg alt.cfg	Invokes the **copy** command associated with the alias *cp*, inserts the *config2.cfg* value in the first parameter position (**%1**) and inserts the *alt.cfg* value in the second parameter (**%2**). The system then invokes the command; it copies the *config2.cfg file on Slot 2 to a new file alt.cfg* on Slot 3.
alias backup "copy 2:%1 3:%1"	Creates an alias named *backup* that takes the first value the user enters when using the alias and inserts it in both parameter positions indicated by **%1** (as shown in the next example).
backup config	Invokes the **copy** command associated with the alias *backup*, inserts the *config* value in the parameter positions indicated by **%1** in the <*alias_value*>, and copies the *config* file from Slot 2 to Slot 3.

Inserting Character Strings in an Alias

The **echo** command prints one or more strings of characters to the Technician Interface console. When the Technician Interface receives the echo request, it sends the accompanying string or strings back to the console. This command is used primarily to accompany system responses to alias commands with meaningful text. This section describes how to issue an **echo** command and how to insert the **echo** command in an alias.

Enter the following command with one or more of the following parameters to submit an echo request.

echo [["]<*string*>["]]

<*string*> is any string of characters.

echo [[**"**]<*string*>[**"**]] [[**"**]<*string*>[**"**]] ...

Double quotes are required only when the string contains one or more spaces or semicolons (;).

Examples:

If you enter:	**The console displays:**
echo hi	`hi`
echo "IP Input Statistics:"	`IP Input Statistics:`
echo Hi hello "How are you?"	`Hi hello How are you?`

To command the system to display a string of characters when responding to an alias command, you insert an **echo** command within the <*alias_value*>.

Surround each <*string*> within the **echo** command with double quotes if the <*string*> contains one or more spaces or semicolons (;). Precede each of the double quotes surrounding the <*string*> with a backslash (\). If you do not use double quotes, insert a backslash before the semicolon that separates the **echo** command from the next command.

Insert **echo \;** to command the system to display blank lines between commands within an <*alias_value*>.

You can also embed parameter references within an **echo** command. Refer to the first example to see how this is done.

Examples:

If you enter:

alias ipstats “echo \; echo \“IP Input Statistics:\”; echo \; get WfIpInterfaceEntry.21.*\; echo \; echo \“IP Output Statistics:\”; echo \; get WfIpInterfaceEntry.24.*”

The system creates an alias named **ipstats** that invokes the commands shown in quotes.

The text wraps as you enter text past column 80. Do not press the return key until you have entered the entire command.

ipstats

The system displays the following:

```
IP Input Statistics:

wfIpInterfaceEntry.wfIpInterfaceInReceives.192.32.6.4.3 = 141501
wfIpInterfaceEntry.wfIpInterfaceInReceives.192.32.15.21.4 = 41304
wfIpInterfaceEntry.wfIpInterfaceInReceives.192.32.16.1.2 = 538
wfIpInterfaceEntry.wfIpInterfaceInReceives.192.32.243.2.1 = 130137

IP Output Statistics:

wfIpInterfaceEntry.wfIpInterfaceForwDatagrams.192.32.6.4.3 = 149189
wfIpInterfaceEntry.wfIpInterfaceForwDatagrams.192.32.15.21.4 = 28400
wfIpInterfaceEntry.wfIpInterfaceForwDatagrams.192.32.16.1.2 = 1086
wfIpInterfaceEntry.wfIpInterfaceForwDatagrams.192.32.243.2.1 = 120635
```

Debugging Aliases

The **verbose** command allows you to display the commands within an <*alias_value*> as an alias executes. This command is useful for locating syntax errors within the <*alias_value*>.

Enter the following to display the verbose mode:

verbose

If the verbose mode is on, the system displays the commands as they execute. If the verbose mode is off, the system does not display the commands.

Enter the following to change the setting of the verbose mode, where [**on** | **off**] is **on** to display alias commands or **off** to turn off the display:

verbose [**on** | **off**]

Examples:

If you enter:	The system:
verbose	Displays Verbose mode on or Verbose mode off.
verbose on	Displays alias commands when they execute.
verbose off	Does not display alias commands when they execute.

Deleting an Alias from Memory

The **unalias** command removes the specified alias from memory. If you substitute the wildcard character (*) for the alias name, the system removes all aliases from memory. Enter the following to delete aliases from RAM:

unalias [*<alias name>* | *****]

<*alias name*> is the name of the command you want to delete.

***** represents all aliases.

Examples:

If you enter:	The system:
unalias scroll	Deletes the alias named *scroll*.
unalias *	Deletes all aliases from memory.

Saving Aliases to a File

You can copy all aliases residing in RAM to a file on a volume for later retrieval.

Enter the following to create an alias file:

save aliases *<vol>:<filename>*

<*vol*> is the volume that will store the alias file.

<*filename*> is the name of the alias file.

Example:

If you enter:	The system:
save aliases 2:aliases.1	Creates a file named *aliases.1* on volume 2 and copies the aliases from RAM to this file.

Note: The command **alias** precedes the alias name and alias text for each entry in the file, allowing you to run the file as a script file.

Loading Aliases from a File

You can use the **source aliases** command to load the aliases from a file residing on the volume to active RAM. The aliases already residing in memory remain in memory; however, the system overwrites any aliases in memory that have duplicate names. Use the **unalias *** command if you want to delete all aliases from memory before entering the **source aliases** command.

Enter the following to load aliases:

source aliases *<vol>:<filename>*

<vol> is the volume storing the alias file.

<filename> is the name of the file that contains aliases.

Example:

If you enter:	The system:
source aliases 2:aliases.1 or **run 2:aliases.1** or **source 2:aliases.1**	Loads the aliases contained in the *aliases.1* file, which is stored on Volume 2.

Note: With Version 7.70 or later router software running, you can use the **source aliases** command to load alias files created in any version of Series 7 or later router software. You cannot, however, use earlier releases of router software to read alias files created with Version 7.70 or later software.

Debugging with Predefined Aliases

This section describes how to use aliases that are useful for debugging common network problems. These aliases are located in the *debug.al* file.

Enter the following to load the aliases that are predefined for debugging, where <*vol*> is the volume containing the files from Bay Networks:

source aliases <*vol*>**:debug.al**

Note: You can also use **run** <*vol*>:**debug.al**.

Table 9-1 shows each alias and its associated function. To invoke an alias, enter the alias after the Technician Interface prompt. Follow the alias with a space and the parameter indicated, if applicable. The console displays the data associated with the alias.

You can display the commands associated with an alias loaded in memory in two ways:

- You can use the **alias** command to display the commands without invoking them.
- You can use the **verbose** command to display the commands associated with an alias whenever an alias executes.

Examples:

Table 9-1. Aliases for Debugging Network Problems

If you enter:	The system:
at_intf <*circuit*> [**1** | **2**]	Enables or disables a circuit. Valid values are 1 = Enable circuit 2 = Disable circuit
at_if <*circuit_no*>	Retrieves configuration information and statistics for the selected circuit.
at_addr	Lists the AppleTalk addresses for the AppleTalk interfaces on the router.
at_cfg	Displays the configured network start, network end, and default zone for all AppleTalk interfaces.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
at_cur	Displays the current network start, network end, and default zone for all AppleTalk interfaces.
at_it	Displays the status of all AppleTalk interfaces.
at_rt	Displays the entries in the routing table, including the node and network IDs of the next hops in the network, the number of hops, and the status of the network.
at_zones	Lists the zones in the router's zone table.
at_arp	Lists the AARP entries in the router's address mapping table.
bgpenabled	Displays the state of all configured BGP connections. Valid values are 1 = Enabled 2 = Disabled
bgppeers	Displays the BGP IDs (for the connections that are established) of all BGP peers.
bgppeerstate	Displays the administrative state of all configured BGP connections. Valid values are 1 = Up 2 = Down 3 = Init 4 = Invalid 5 = NotPresent
bgpconnstate	Displays the *BGP FSM* state of all configured BGP connections. Valid values are 1 = Idle 2 = Connect 3 = Active 4 = OpenSent 5 = OpenConfirm 6 = Established
bgp3origin	Displays the *ORIGIN* attribute of each network advertisement received via BGP-3. Valid values are 1 = IGP 2 = EGP 3 = Incomplete
bgp3aspath	Displays the *AS_PATH* attribute of each network advertisement received via BGP-3.
bgp3nexthop	Displays the *NEXT_HOP* attribute of each network advertisement received via BGP-3.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
bgp3metric	Displays the *INTER_AS_METRIC* attribute of each network advertisement received via BGP-3.
cctnames	Displays all circuit names.
ccttypes	Displays all circuits and their types. The types are as follows: 10 = CSMACD 20 = SYNC 30 = T1 40 = E1 50 = Token 60 = FDDI
decadjs	Displays all DECnet adjacent nodes and their respective adjacency table indexes. The following example shows one line in the display, where 6145 is the index, 2 is the area, and 3 is the node: `wfivAdjEntry.wfivAdjNodeAddr.6145 = "2.3"`
decadj *<index>*	Displays DECnet adjacency information about the index you enter. You can obtain the <*index*> by using the **decadjs** alias.
decarts	Displays all known DECnet areas and the next hop to each of these areas.
decarinf *<area>*	Displays DECnet area information for the area you enter.
decbase	Displays DECnet global configuration parameters (base record).
decdr	Displays the designated router address for each DECnet interface.
decnrts	Displays DECnet Level 1 routing node information.
decninf *<area.node>*	Displays DECnet information about the node whose area and node number you enter.
decifs	Displays node and area configuration, and interface indexes for all interfaces running DECnet.
decif *<index>*	Displays DECnet information for the interface index you enter. You can obtain the <*index*> by using the **decifs** alias.
decpri	Displays DECnet circuit priorities for all interfaces.
deccost	Displays DECnet circuit costs for all interfaces.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
decstats	Displays all DECnet receive, transmit, and dropped statistics.
enetstats	Displays all Ethernet receive and transmit statistics.
fddior *<circuit_no.>*	Displays the number of FDDI octets received for the specified circuit.
fddifr *<circuit_no.>*	Displays the number of FDDI frames received for the specified circuit.
fddiot *<circuit_no.>*	Displays the number of FDDI octets transmitted for the specified circuit.
fddift *<circuit_no.>*	Displays the number of FDDI frames transmitted for the specified circuit.
fddi_stats	Displays all FDDI receive and transmit packet statistics.
fddistat *<circuit_no.>*	Displays the state of the FDDI circuit.
fddistats *<circuit_no.>*	Displays all FDDI receive and transmit packet statistics for the specified circuit.
hwslot *<slot_no.>*	Displays hardware information for the associated slot. This includes the serial number and revision level.
fr_dlcmi *<line.llindex>*	Lists all MIB attributes for the DLCMI entry of the specified Frame Relay interface.
fr_enable_ad *<line.llindex>*	Enables the Annex D Data Link Control Management interface on the specified Frame Relay interface.
fr_enable_lmi *<line.llindex>*	Enables the LMI Data Link Control Management interface on the specified Frame Relay interface.
fr_enable_none *<line.llindex>*	Disables all DLCMI functions for the specified Frame Relay interface.
fr_info	Lists all configured Frame Relay interfaces and their instance IDs (*line.llindex*).
fr_mgttype *<line.llindex>*	Displays the management type selected for the specified Frame Relay interface.
fr_status *<line.llindex>*	Displays the status of the specified Frame Relay interface.
fr_vcs	Lists all instances (configured PVCs) in the Frame Relay virtual circuit table.
fr_vc *<line.llindex.dlci>*	Lists all MIB attributes for the virtual circuit table of the specified Frame Relay PVC.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
hwmods	Displays slots and their associated hardware module IDs.
hwnode	Displays the serial number and revision level of router.
ipfwd	Displays the age of each entry in the IP forwarding table.
ipfwdage	Displays the age of each entry in the IP forwarding table.
ipfwdas	Displays the next hop AS of each entry in the IP forwarding table.
ipfwdmetric	Displays the metric of each entry in the IP forwarding table.
iproutes	Displays all IP networks that are known and the next hop.
iphops	Displays all IP networks that are known and their associated hop counts.
iphosts	Displays all configured adjacent IP hosts.
iparp	Displays all MAC addresses and associated ARP addresses in the router's ARP cache.
ipifs	Displays all IP interfaces and their associated indexes.
ipif *<address.index>*	Displays all IP information for the IP interface address you enter. For example, enter the following where 192.32.10.10 is the first interface: **ipif 192.32.10.10.1** You can obtain the <address.index> by using the **ipifs** alias.
ipsroutes	Displays all IP static routes configured in the node.
ipstats	Displays all IP receive and IP transmit packet statistics.
ipx_intf	Enables or disables a specific IPX interface. 1 = Enable 2 = Disable
ipx_if *<interface_ID>*	Displays the IPX interface record for the specified interface ID.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
ipx_route *<instance_ID>*	Displays the IPX route record for the instance ID of the particular route you specify.
ipx_server *<instance_ID>*	Displays the IPX server table for the instance ID of the particular server you specify.
ipx_it	Displays the IPX interface table, including the state of the interfaces. The states are 1 = Up 2 = Down
ipx_rt	Displays the metrics of all routes.
ipx_st	Displays the names of all servers.
ipxinr *<interface_ID>*	Displays the number of packets received on a specific interface.
ipxind *<interface_ID>*	Displays the number of packets (RIP or SAP) received on a specific interface.
ipxforwd *<interface_ID>*	Displays the number of packets forwarded on a specific interface.
ipxoutr *<interface_ID>*	Displays the number of out requests (RIPs and SAPs originated from the router) for the interface you specify.
ipx_stat *<interface_ID>*	Displays the last four aliases on the interface you specify.
ipx_nexthop *<instance_ID>*	Displays the next hop for the network you specify.
lbbase	Displays all (Learning) bridge global configuration parameters (base record).
lbfwd	Displays all node MAC addresses in the bridge's forwarding table.
lbif *<index>*	Displays bridge information for the interface index you enter. You can obtain the *<index>* by using the **lbstate** alias.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
lbstate	Displays bridge interfaces and their current states. The following example shows one line in the list of interfaces, where 1 is the index and 2 is the state: `wfBrTpInterfaceEntry.wfBrTpInterfaceState.1 = 2` The states are 1 = Up 2 = Down 3 = Init 4 = Not present
lbstats	Displays bridge receive, transmit, and dropped packet statistics.

mem_info *<slot_no.>*	Displays the specified slot's total physical memory and the memory allocation for the local and global memory pools, in KB. For example, if you enter mem_info 2, the system displays information similar to the following:
	
	`Memory information for slot 2:`
	`wfKernParamEntry.wfKernParamTotMem.2=8192`
	`wfKernParamEntry.wfKernParamLocMem.2=6144`
	`wfKernParamEntry.wfKernParamGlobMem.2=2048`

osiadjs	Displays the adj ID.
osil1lsp	Displays the LSP ID for Level 1.
osil2lsp	Displays the LSP ID for Level 2.
osil1routes	Displays the path or router ID for Level 1.
osil2routes	Displays the path or router ID for Level 2.
ospf_drs	Reports the designated router and backup designated router for each of the router's attached OSPF networks.
ospf_intf	Reports the state of all the router's OSPF interfaces, including virtual links. The states are 1 = Down 2 = Loopback 3 = Waiting 4 = Point to point 5 = Designated router 6 = Backup designated router 7 = Other designated router

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
ospf_lsdb	Lists all interfaces in the link-state database.
ospf_nbrs	Reports the state of every OSPF neighbor that the router knows about. The states are 1 = Down 2 = Attempt 3 = Init 4 = Two way 5 = Exchange start 6 = Exchange 7 = Loading 8 = Full
protocols	Displays bit map in decimal form representing all protocols running and their associated slots.
setvol *<slot_no.>*	Sets the active volume for TFTP (puts and gets).
shovol	Displays the current active volume for TFTP (puts and gets).
snmpbase	Displays all SNMP configuration parameters (base record).
sr_intf *<instance_ID>*	Enables or disables Source Routing for a specific interface. 1 = Enable 2 = Disable
sr_info	Displays the contents of the Source Routing database record.
sr_cctstats *<circuit_no.>*	Displays the status of the specified circuit.
stid	Displays the Spanning Tree node identifier.
stif *<index>*	Displays all Spanning Tree bridge information for the (Learning) bridge interface index you enter. You can obtain the *<index>* by using the **lbstate** alias.
stroot	Displays the Spanning Tree designated root node identifier.

Table 9-1. Aliases for Debugging Network Problems *(continued)*

If you enter:	The system:
ststate	Displays the current state of each link running the Spanning Tree protocol in the node. The states are 1 = Disabled 2 = Blocking 3 = Listening 4 = Learning 5 = Forwarding 6 = Broken
todec *<hex_no.>*	Converts the specified hexadecimal number to decimal. A hexadecimal number begins with *0x* (for example, *0x1234*).
tohex *<decimal_no.>*	Converts the specified decimal number to hexadecimal.
trrxo *<circuit_no.>*	Displays the number of Token Ring octets received for the specified circuit.
trrxf *<circuit_no.>*	Displays the number of Token Ring frames received for the specified circuit.
trtxo *<circuit_no.>*	Displays the number of Token Ring octets transmitted for the specified circuit.
trtxf *<circuit_no.>*	Displays the number of Token Ring frames transmitted for the specified circuit.
tr_stats *<circuit_no.>*	Displays all Token Ring receive and transmit packet statistics for the specified circuit.
trs *<circuit_no.>*	Displays the state of the Token Ring circuit.
vines_info *<router_ID>*	Displays the information contained in the VINES database record for the specified router.
vines_ID *<router_ID>*	Displays the VINES network number of the router.
vines_nbrs	Displays the contents of the VINES Table of Neighbors.
vines_nets	Displays the contents of the VINES Table of Networks.
vines_nexthops	Displays the contents of the VINES Table of Next Hops.
vines_cctstats *<circuit_no.>*	Displays VINES statistics for a specified circuit.
vines_client_en	Enables VINES clients.

Appendix A
Using the Bay Networks Router MIB

This appendix describes how to use the Bay Networks router Management Information Base (MIB). The Bay Networks router MIB is a proprietary database that contains configuration parameters and statistics. You use the Bay Networks router MIB to obtain and change configuration parameters and statistics through the Technician Interface or through network management software. This appendix provides

- An overview of the structure of the Bay Networks router MIB
- A description of the Bay Networks router MIB files
- Specifications with which the Bay Networks router MIB complies
- Implementation notes

Overview

This section examines the structure of the Bay Networks router MIB. The object tree assigned to the Bay Networks router MIB is as follows:

iso.org.dod.internet.private.enterprises.wellfleet

The corresponding numeric identifier assigned to the Bay Networks router MIB subtree is as follows:

1.3.6.1.4.1.18

Figure A-1 shows an example of the hierarchy of objects. The prefix that precedes each object name identifies a Bay Networks enterprise-specific object.

The wfSwSeries7 (wellfleet.3) object names and identifies the Bay Networks router MIB for the Series 7 and later software. The nodes in the first level below wfSwSeries7 are as follows:

- wfHardwareConfig (wfSwSeries7.1) contains the objects that pertain to the hardware configuration.
- wfSoftwareConfig (wfSwSeries7.2) contains the objects that pertain to software that is loaded, such as protocols and drivers, and information required for loading, such as where in memory a driver gets loaded.
- wfSystem (wfSwSeries7.3) contains the objects that pertain to the system record, console, remote console, and the circuit name table.
- wfLine (wfSwSeries7.4) contains the objects that determine the functioning of the drivers that control the data-link layer media.
- wfApplication (wfSwSeries7.5) contains the protocol applications.

Figure A-1. Sample Top-Level Hierarchy of the Bay Networks Router MIB

wfLine (wfSwSeries7.4)
- wfCSMACDTable (wfLine.1)
- wfWfTokenRingTable (wfLine.2)
- wfAsyncTable (wfLine.3)
- wfFddiTable (wfLine.4)
- wfSyncTable (wfLine.5)
- wfHwFGroup (wfLine.6)
- wfHssiTable (wfLine.7)
- wfMcT1Group (wfLine.8)
- wfDS1E1Group (wfLine.9)
- wfDs1Group (wfLine.12)
- wfDs3Group (wfLine.13)
- wfSipGroup (wfLine.14)
  - wfSipPlcpGroup (wfSipGroup.2)
- wfFddiGroup (wfLine.15)
  - wfFddiSmtGroup (wfFddiGroup.1)
  - wfFddiMacGroup (wfFddiGroup.2)
  - wfFddiPathGroup (wfFddiGroup.3)
  - wfFddiPortGroup (wfFddiGroup.4)
- wfCSMACDAutoNegGroup (wfLine.16)
- wfPktCaptureGroup (wfLine.21)
- wfCompressionGroup (wfLine.22)
- wfAtmInterfaceGroup (wfLine.23)
  - wfAtmCommonGroup (wfAtmInterfaceGroup.1)
  - wfAtmLinkModuleGroup (wfAtmInterfaceGroup.2)
  - wfAtmCellSwitchGroup (wfAtmInterfaceGroup.3)
- wfSonetGroup (wfLine.24)
- wfDsx3Group (wfLine.26)
- wfBisyncGroup (wfLine.27)

Figure A-1. Sample Top-Level Hierarchy of the Bay Networks Router MIB (*continued*)

Figure A-1. Sample Top-Level Hierarchy of the Bay Networks Router MIB *(continued)*

wfInternet *(continued)*
- wfBootpGroup (wfInternet.8)
  - wfBootpClientGroup (wfBootpGroup.1)
  - wfBootpServerGroup (wfBootpGroup.2)
  - wfBootpRelayAgentGroup (wfBootpGroup.3)
- wfRarpGroup (wfInternet.9)
- wfFtpGroup (wfInternet.10)
- wfNetBIOSIpGroup (wfInternet.11)
- wfDvmrpGroup (wfInternet.12)
- wfIgmpGroup (wfInternet.13)
- wfPimGroup (wfInternet.14)
- wfIpv6Group (wfInternet.16)

wfAppletalkGroup (wfApplication.4)
wfIpxGroup (wfApplication.5)
wfOsiGroup (wfApplication.6)
wfVinesGroup (wfApplication.8)
wfWanGroup (wfApplication.9)
- wfFrameRelayGroup (wfWanGroup.1)
- wfPppGroup (wfWanGroup.2)
- wfX25Group (wfWanGroup.4)
- wfAtmGroup (wfWanGroup.5)
  - wfAtmLeGroup (wfAtmGroup.20)
- wfFrswGroup (wfWanGroup.6)
- wfSmdsSwGroup (wfWanGroup.7)
- wfIsdnGroup (wfWanGroup.8)
- wfFrameRelay2Group (wfWanGroup.9)

wfXnsGroup (wfApplication.10)
wfLanManagerGroup (wfApplication.12)
wfAppnGroup (wfApplication.14)
wfIpexGroup (wfApplication.15)
wfIntegratedServicesGroup (wfApplication.16)
wfRRedGroup (wfApplication.17)
wfBotGroup (wfApplication.18)
wfAccountingGroup (wfApplication.20)

Figure A-1. Sample Top-Level Hierarchy of Bay Networks Router MIB Objects *(continued)*

Bay Networks Router MIB Files

A collection of ASCII files (one per router entity) together describe the Bay Networks router MIB. These files load automatically onto the Site Manager workstation or PC when you install the Site Manager software. The Site Manager software modules read these files during startup.

Site Manager installs these files at *\wf\mibs* on PCs, and at */usr/wf/mibs* on UNIX workstations. For example, the path to the PPP mib definition file on a UNIX workstation is */usr/wf/mibs/ppp.mib.*

If you want to load these MIB files into a local MIB browser tool, first load the file *wfcommon.mib*; otherwise, you may experience errors using the browser tool.

Caution: If you want to open any MIB file with an ASCII text editor, do so with read-only protection enabled. This should eliminate the possibility of corrupting (over-writing) the contents of that file.

Compliance with Specifications

The Bay Networks router MIB complies with the standards described in the following documents, with the exceptions noted in the "Implementation Notes" section.

- *Concise MIB Definitions* (RFC 1212)
- *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II* (RFC 1213)
- *Structure and Identification of Management Information for TCP/IP-Based Internets* (SMI; RFC 1155)
- *Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One* (ISO 8824)

Also, the latest editions of the following textbooks provide information about these standards:

- Comer, Douglas E. *Internetworking with TCP/IP, Vol. 1*. Englewood Cliffs, New Jersey: Prentice-Hall.
- Rose, Marshall T. *The Simple Book*. Englewood Cliffs, New Jersey: Prentice-Hall.
- Stevens, Richard W. *TCP/IP Illustrated, Vol. 1*. Reading, Massachusetts: Addison-Wesley.

Implementation Notes

The following notes list the assumptions made about MIB-II object definitions, supported traps, unsupported objects, and unsupported operations.

MIB-II Object Definitions

The assumptions about MIB-II object definitions are as follows:

ifNumber	Represents the total number of rows in the interface table.
ifIndex	Represents a unique integer corresponding to a data-link layer entity. ifIndex values are derived from Bay Networks circuit numbers. A single interface or a group of interfaces (multiline) can be a member of a single circuit. With a single interface, a single ifIndex value matching the circuit number is allocated and the ifTable statistics correspond to the single interface. With a group of interfaces, a single ifIndex value is still allocated; however the ifTable statistics are aggregated for all interfaces in the circuit group. Four statistics require special consideration when using multiline: ifAdminStatus, ifOperStatus, ifMTU, and ifPhysAddress. ifAdminStatus and ifOperStatus return UP if at least one interface is up. All interfaces must be down before DOWN is returned. The ifMTU value returned is the minimum MTU for the circuit group and the ifPhysAddress is the physical address of the first interface in the circuit to initialize.

ifSpecific	The object identifier that points to an instance of the first conceptual column in the appropriate proprietary media MIB.
ipAddrEntry	In certain circumstances, the index to this table, ipAdEntAddr, may not be sufficient to uniquely identify a particular instance. In these situations, the attribute ipAdEntIfIndex is appended to the instance identifier for subsequent entries with the same index.
ipRouteEntry	The instance identifier for the MIB-II routing table, ipRouteDest, is insufficient to uniquely identify all possible routes to a given destination. The MIB-II routing table, therefore, contains only a representative sample of the total routing table. For a more accurate description of the system's IP routes, see wfIpForward Entry (1.3.6.1.4.1.18.3.5.3.2.1.16.1), which is indexed by destination address, destination subnet mask, route source, policy, and next-hop address.

Supported Traps

The following generic traps are supported by the software:

coldStart	Issued when the network management entity initializes. The cold-start trap is delayed up to 30 seconds to give the network interfaces time to initialize, thus improving the chances that the trap will be received by all the registered managers of this device.
warmStart	Issued when the management protocol is re-enabled after being disabled.
linkUp	Issued when an interface has been initialized and is providing service to upper layers. Note that during system initialization, the transmission of link traps may be masked because the network layer may not be fully initialized and ready to send traps.
linkDown	Issued when an interface is no longer providing service.

authenticationFailure	Issued when an SNMP access occurs. An invalid access occurs if a bad community or illegal manager address is used. Authentication traps will be masked if they are not enabled.
egpNeighborLoss	Issued when an acquired EGP neighbor is lost.
enterpriseSpecific	All Bay Networks router system log events can be sent as traps. They must be configured through the wfSnmpTrapEntityTable and the wfSnmpTrapEventTable. The specific trap value is a four-byte value. The first (most significant) byte indicates the slot generating the event; the second byte indicates the severity [debug (1), informational (2), warning (4), fault (8), and trace (16)]; the third byte indicates an entity code (for example, ip (2), snmp (3), csmacd (9); and the fourth byte indicates the event number or the particular event type unique to each entity. The specific traps contain one variable binding -- a display string with the name 1.3.6.1.4.1.18.3.5.3.5.4.1.0. The string contains the actual log message that was recorded in the system event log.

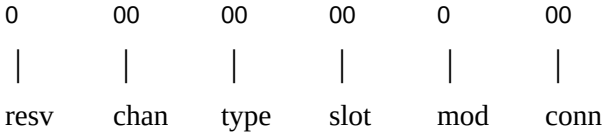
Unsupported Operations

The SNMP **set** operation is not supported for MIB-II objects. All **set** operations must be performed through the Bay Networks private MIB (1.3.6.1.4.1.18.3).

Line Number Attributes

Line number attributes exist in all line records (for example: SYNC,HSSI, CSMACD, and TOKEN) in the Bay Networks router MIB for Version 9.00 router software. These attributes have the name wfXyzLineNumber, where *Xyz* is the prefix for the appropriate line record. Site Manager generates a line number attribute to uniquely identify each port in the router configuration. The router uses line numbers to accommodate more than one line per port, and to reference WAN protocols configured on those lines.

The line number encodes several attributes of the line it represents. You can use Technician Interface **list** and **get** commands to examine and decode a line number. The individual fields of the number correspond to different attributes of a line, as follows:



Field	Purpose
resv. (0-1)	Reserved for future expansion, with a default value of 0.
chan (0-99)	Indexes multiple lines over one connector, such as on the MCT1 board. This is equivalent to “channel” for MIB objects using “slot.conn.chan” format. For boards that support only 1 line per connector, chan = 0.
type (0-99)	The interface type identifier (for example: CSMACD and SYNC). These are the same as the constants defined in the CCT_NAME portion of the MIB. For example: CIRCUIT_TYPE_CSMACD (1-10) CIRCUIT_TYPE_SYNC (2-20) CIRCUIT_TYPE_T1 (3-30) CIRCUIT_TYPE_E1 (4-40) CIRCUIT_TYPE_TOKEN (5-50) CIRCUIT_TYPE_FDDI (6-60) CIRCUIT_TYPE_HSSI (7-70)
slot (1-99)	For most Bay Networks routers, each numbered slot holds a CPU module and a link module. For model ASN routers, this number represents the chassis unit identifier (which contains a CPU and drives up to four link modules). You set the ASN slot number by means of a thumbwheel on the chassis. The thumbwheel has settings that range from 1 to 4.
mod (1-9)	The module number has a default value of 1 on most Bay Networks routers, which corresponds to the first (only) module on a slot. The “mod” can be any number from 1 to 9 for a model ASN router, where one CPU supports up to four link modules.
conn (1-16)	Connector number for a given media. It is given 2 digits to accommodate 16 port boards.

Example:

Line number = 102101

- chan = 1
- type = 0
- slot = 2
- mod = 1
- conn = 01

This is the only line on the first CSMACD connector on module 1 of slot 2.

Appendix B
Using Out-of-Band Access to Transfer Files

This appendix describes how to use the **xmodem** command to perform out-of-band file transfers. The **xmodem** command enables you to transfer files between remote workstations and Bay Networks routers when all IP routing paths between them are down. You cannot use the **xmodem** command to transfer files between Bay Networks routers.

Overview

Both UNIX and 386/486 DOS remote workstations allow you to log in to the Technician Interface port of a router and enter **xmodem** commands. However, each type of workstation uses a different utility program for opening and closing out-of-band (dial) connections between workstation and router.

With a Sun workstation, you initially establish a connection by configuring and running the Terminal Interface Program (TIP). The program has two associated files, */etc/phones* and */etc/remote*, in which you can enter setup information such as the telephone number of a remote router (*/etc/phones*) and modem interface settings (*/etc/remote*). You run the program by entering a **tip** command with appropriate syntax at the UNIX command line prompt.

With a 386/486 DOS workstation, you initially establish a connection by configuring and running the Bay Networks Terminal Program (filename *wfterm*). To run the program, click on the *Wfterm* icon in the display of your Site Manager workstation.

This section describes

- The asynchronous terminal program available on UNIX and 386/486 DOS remote workstations
- The Technician Interface **xmodem** command, its parameters, and its options
- How you use the asynchronous terminal program and **xmodem** commands together in procedures for transferring files to and from Bay Networks routers

About xmodem

Bay Networks routers support **xmodem** as a Technician Interface command and a set of protocols for moving files between the Technician Interface console port of a router and a remote workstation. **xmodem** is based on the Christensen protocol file transfer utility, V3.9, November 1990.

You determine the protocol for the task you need to perform by selecting the appropriate syntax (parameters and options) for each **xmodem** command. You enter **xmodem** commands directly at the command line prompt of either a UNIX workstation or a 386/486 DOS workstation. (The procedural information you need to enter and use **xmodem** commands follows later in this appendix.)

As a set of protocols, **xmodem** includes the

- XMODEM/CRC protocol
- MODEM7 batch protocol
- XMODEM-1K block protocol
- YMODEM batch protocol

Of the four protocols available through **xmodem** commands, *you need to use only the YMODEM batch protocol* to transfer Bay Networks files between a remote workstation and a router. For this reason, this section covers information on the YMODEM protocol only. (For information on the other protocols supported by **xmodem** commands, refer to “For More Information,” later in this appendix.)

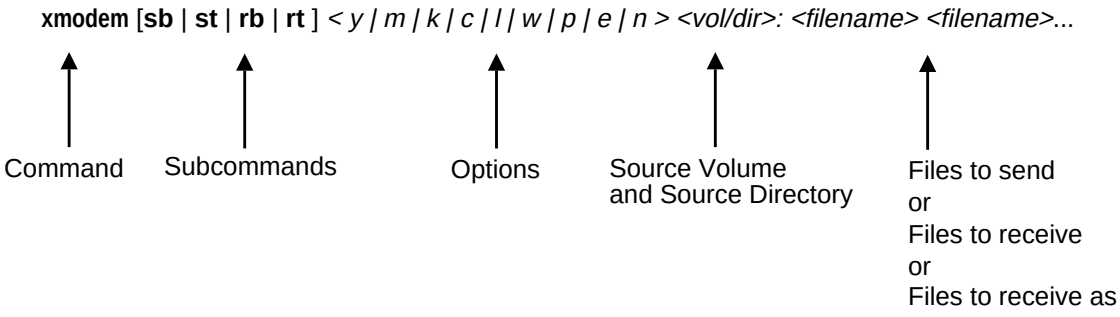
In support of Bay Networks router file management tasks, the YMODEM batch protocol has the following capabilities:

- Supports batch file transfers (moving one or more files specified in a single **xmodem** command)
- Automatically converts filenames received during batch file transfer operations
- Transfers binary files with error detection
- Marks every transferred file with a time stamp, which indicates the most recent modification date of a file
- Automatically deletes a file unsuccessfully transferred between a router and a workstation
- Allows you to cancel a file transfer operation while that operation is still in progress

YMODEM transfers binary files intact, with no padding, and using a default packet size of 128 bytes. To use the YMODEM protocol, a Bay Networks router does not require access (in-band) to the IP network on which a source/destination remote workstation also resides. Instead, you use out-of-band (dial network) access from the UNIX or 386/486 DOS workstation to run Technician Interface **xmodem** commands and conduct file transfers through a modem. You are most likely to use the YMODEM protocol to move files when your IP network is down or impaired.

The xmodem Command

The following represents the syntax of the **xmodem** command:



Note: You can enter the **xmodem** command line parameters and option flag characters in upper- or lower-case. Do not insert spaces between parameter characters, between option flag characters, or between a parameter and an option flag character. Do insert a space character after the last option flag and between filenames (for YMODEM batch file transfers).

For out-of-band file transfer operations, use only the **xmodem** command parameters and options that are appropriate for

- The YMODEM protocol
- The type of file you need to transfer

The relevant **xmodem** command *parameters* are **sb** (send binary) and **rb** (receive binary). The relevant *option flags* are **y** (ymodem), **l** (logging), **w** (wait before initiating transfer), **p** (print/display **xmodem** information and events), **n** (allow midtransfer cancel), and **e** (disable EOT verification -- DOS only).

The **y** and **w** option flags are required in the **xmodem** commands (to select YMODEM, and for proper handshaking with the YMODEM protocol program running on the remote workstation). You should use the **p** option to monitor the progress of any out-of-band file transfer in progress (UNIX only).

You can enable or disable logging of **xmodem** events by means of the **l** flag, or cancel a particular file transfer by entering control-x.

Command Parameters

When you enter an **xmodem** command at the Technician Interface command line prompt, follow the entry with *only one* of the following parameters:

Parameter	Name	Meaning or Action
sb	Send Binary	Sends files as they exist on disk or in Flash memory, without conversion.
st	Send Text	Sends ASCII text files.
rb	Receive Binary	Places files on disk or in Flash memory, without conversion. YMODEM silently destroys existing files of the same name.
rt	Receive Text	Receives ASCII text files.

Command Options

After you enter the **xmodem** command parameter that is appropriate for the operation you need to perform (**sb**/**rb**), enter

- The **y** option flag for any send binary or send receive operation
- The **w** option flag for any send binary operation
- The **p** option flag for any **xmodem** command you use to set the UNIX workstation in either send binary or receive binary mode
- The **e** option flag for any **xmodem** command you use to transfer files to the router using the Windows Terminal program

The **xmodem** option flags relevant to the use of the YMODEM single- or batch-file transfer protocol have the meanings shown in Table B-1.

Table B-1. Xmodem Option Flags

Option Flag	Meaning or Action
y	Selects the YMODEM batch protocol for sending files. Sends in sequence any list of files you specify in the Technician Interface command line.
m	Selects the MODEM7 batch protocol for sending files.
k	Uses 1 kB packets on transmit.
c	Selects CRC mode on receive.
w	Causes the Technician Interface to wait 15 seconds before initiating the startup handshake, which in turn commences the specified file transfer operation. If you are using a 386/486 DOS PC as a workstation, you trigger the initial handshake by selecting Ymodem-Send or Ymodem-Receive from the File Transfers pull-down menu.
l	When specified in the command line, l inhibits the logging of YMODEM events in the system log. (Automatic logging is a default mechanism of the XMODEM/YMODEM protocols.) When you enable logging (by not specifying the l flag in the command line), log messages for significant events, errors, and retries are sent to the system log. The log messages can be useful for troubleshooting.
p	Prints (displays) information and events pertaining to the YMODEM batch file transfer in progress (UNIX only).
n	Allows CAN-CAN (^x^x) aborts during midtransfer. Otherwise, the YMODEM protocol allows CAN-CAN aborts only at the beginning of a file transfer operation.
e	Disables EOT verification when transferring files to the router (DOS only).

Filenames

The conventions for the treatment of filenames by the YMODEM protocol are

- The source router or the remote workstation sends files with path names stripped and limited to eight characters plus a three-character extension. The router or workstation converts all filename characters to lower case, and all ":" characters to "/" characters.
- The target router or workstation stores received files under their transmitted names. However, YMODEM converts / characters in the received filename back into : characters. YMODEM also translates all uppercase characters into lowercase, and eliminates any trailing dots in the filename.
- If you want to specify multiple filenames in a single **xmodem** command (that is, a YMODEM batch file transfer operation), insert a space after every filename except for the last name you specify in the command line. You can also use wildcards in a filename (for example, **.bat*).

For More Information

The following book provides additional information about **xmodem** protocols:

Forsberg, Charles. Ed. *XMODEM/YMODEM Protocol Reference*.

Implementation Notes

This section provides implementation notes on

- How **xmodem** handles files and checks for errors in files
- How **xmodem** responds when you cancel a file transfer operation
- How to manage modem hardware incompatibilities
- How to view **xmodem** log events

File Handling

The following information applies to configuration files you transfer between a remote workstation and a Bay Networks router:

- The YMODEM protocol truncates binary files *received* in a batch transfer operation. The YMODEM header specifies the truncated size.
- YMODEM sets the file modification timestamp field in the header of all *transmitted* binary files. Note, however, that the timestamp is subject to a specific time-zone reference.

Error Checking

YMODEM performs the following error checks on file transfers between remote workstations and Bay Networks routers:

- If YMODEM detects 10 or more errors during the transmission or reception of any one packet, it cancels the transfer in progress.
- If an unexpected error occurs before a file is completely received, YMODEM deletes the incomplete file.

Canceling a File Transfer

While waiting for the beginning of a file transfer, YMODEM treats two CAN (control-x) characters received within 3 seconds of each other as a request to cancel the operation. CAN characters do not cancel the operation if received while a transfer is in progress, unless you specify the **n** option flag in the Technician Interface **xmodem** command line.

Modem Interface Differences

If you are not using a Hayes compatible modem locally attached to your workstation, you may need to follow interface line control procedures appropriate for that modem. Such procedures may be necessary if, for example, quitting the terminal interface program (for example, **tip** or *Wfterm*) fails to switch the modem to an on-hook state. Going on-hook should cause the dialed connection between the local and the remote modems to be dropped.

You may also encounter differences in modem interface cabling requirements.

For more detailed information on these and other modem-related issues, refer to the user manual for the modem you want to use for Technician Interface access.

Viewing xmodem Log Events

To view the log information for **xmodem** (YMODEM) file transfers, enter the following command at the Technician Interface command line prompt:

log -eXMODEM -fdi

Hardware Configuration

To transfer files out-of-band between any Bay Networks router and a remote workstation, you use the hardware configuration shown in Figure B-1.

Figure B-1 shows how to connect a Bay Networks router and workstation to a dial network using two Hayes compatible modems. With this configuration, you use a remote PC or UNIX workstation. The configuration supports a remote connection to the router's Technician Interface.

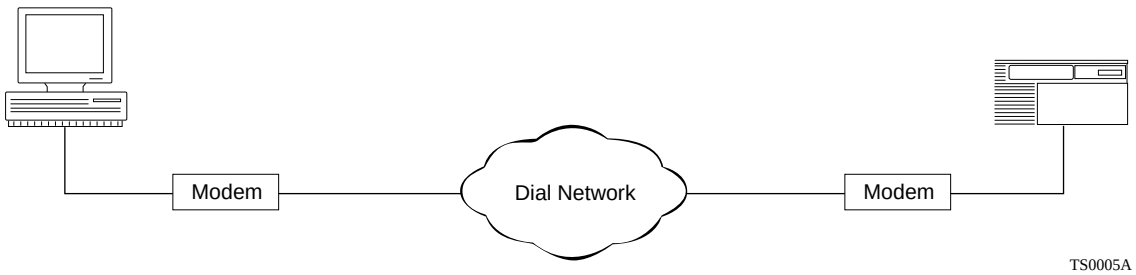


Figure B-1. Modem Connection

Note: Use a network interface cable to connect a modem to the dial network. Use an RS-232-C modem cable to connect a workstation or Bay Networks router to a modem. (Use cable No. 7825 for all except BLN, BLN-2, and BCN routers. Use cable No. 77850 only for BLN, BLN-2, and BCN routers.)

Out-of-Band File Transfers from a UNIX Workstation

This section provides the procedures you need to

- Open a dial connection between your workstation and a specific router
- Transfer files to or from a router
- Close (hang up) the connection between the workstation and router

Opening a Connection

On a SunOS platform, you can use the Terminal Interface Program or **tip** command to

- Establish a connection to the Technician Interface port of a router
- Initiate file transfers to and from the router
- Close the connection between the remote workstation and the router

For detailed information on how to set up and use **tip** and its related files (*/etc/phones* and */etc/remote*) on a Sun workstation, enter **man tip** at the UNIX command line prompt. The workstation should respond by displaying all of the information that is available on **tip** in the UNIX online command reference manual. You enter modem interface settings into the */etc/remote* file. You enter dial information (a telephone number) in the */etc/phones* file.

Transferring Files from Router to UNIX Workstation

To transfer one or more files from a Bay Networks router to your UNIX workstation, use the following procedure:

1. **At the UNIX command line prompt, enter a cd command to change from the current directory to the directory that should receive the files you want to transfer from the router.**
2. **Enter a tip command on the workstation to open a dial connection between the workstation and the desired router. For example,**

   tip modem0

   modem0 designates the workstation port that accommodates the dial modem attached to the workstation. The system displays the following message:

   ```
   Connected
   ```

3. **Press return to invoke the Technician Interface login prompt from the target router. The system displays the following prompt:**

   ```
   Login:
   ```

4. **Enter Manager and a password, if necessary, to log in to the router's Technician Interface. The system displays the following message and prompt:**

   ```
   Welcome to the <node type> Technician Interface.
   $
   ```

5. **Enter a cd command to designate the disk volume or memory card "volume" that contains the files you want to transfer to your UNIX workstation. For example:**

   cd a: (designates diskette Volume a)

   or

   cd 2: (designates a memory card volume in router Slot 2)

6. **Enter a dir command (if necessary) to view the list of files in the volume/ memory card. The system displays a screen similar to the following table:**

File Name	Size	Date	Day	Time
abc.cfg	1814	10/28/94	Thurs.	10:29:06
def.cfg	2293	11/03/94	Wed.	17:16:29
ghi.cfg	4197	11/15/94	Mon.	08:34:04

7. **Determine which files you need to transfer from the router to the workstation.**

8. **Enter the xmodem send binary command, as follows:**

   xmodem sby *<source_vol>*: *<filename> . . . <filename>*

   sb is a send binary file.

   y is the YMODEM file transfer option.

   <*source_vol*> is either a slot number of a memory card or the letter of the disk drive volume that contains the files you want to send to the workstation.

   <*filename*> is the name of the file you want to send from the router to the workstation. If you want to enter multiple filenames as part of a YMODEM batch file transfer operation, insert a space character between the filenames. (For more information on Technician Interface filename specifications, refer to Chapters 4 and 5.)

9. **Type ~c (tilde-c) to escape momentarily from the Technician Interface command line prompt to the UNIX workstation command line prompt. The workstation responds**

   ```
   Local command?
   ```

10. **Enter an xmodem receive binary command with the print (display) transfer events and information option flag (p) set in the command line, as follows:**

    xmodem rbyp *<filename> . . . <filename>*

    rb is a receive binary file.

    y is the YMODEM file transfer option.

    p prints (displays) important information and events pertaining to the file transfer(s) you are about to initiate.

    <*filename*> . . .<*filename*> = The (optional) filenames you want to assign to files when they reach the workstation.

    Pressing return to execute the **xmodem** command triggers the necessary handshakes between the YMODEM protocol program running on the workstation and the YMODEM program running on the router. This handshaking in turn triggers the start of the file transfers you specified in the **xmodem** command entered at the Technician Interface command line prompt.

Workstation and router response: (typical)

```
-----------------

XMODEM File Receive Function

CRC mode requested on command line

YMODEM Batch Protocol

YMODEM Batch Receive Complete
```

`away for 37 seconds` (the amount of time the router's Technician Interface relinquished control to the router's YMODEM protocol program; i.e., the duration of the file transfer operation)

```
!

$
```

11. **If you are finished transferring files from the router to the remote workstation, enter `logout` at the Technician Interface command line prompt.**

    This action returns control to the UNIX workstation command line prompt.

12. **Enter the `ls` command to list the contents of the current (receiving) directory, to verify that the file transfer operation completed successfully.**

Transferring Files from UNIX Workstation to Router

To transfer one or more files from your UNIX remote workstation to a Bay Networks router, use the following procedure:

1. **At the UNIX command line prompt, enter a `cd` command to change (if necessary) from the current directory to the directory that contains the files you want to transfer to the router.**
2. **Enter a `dir` command (if necessary) to view the list of files in the directory.**
3. **Determine which files you need to transfer from the workstation to the router.**
4. **Enter a `tip` command on the workstation to open a dial connection between the workstation and the desired router. For example:**

   `tip modem0`

   `modem0` designates the workstation port that accommodates the dial modem attached to the workstation. The system displays the following message:

   ```
   Connected
   ```

5. **Press return to invoke the Technician Interface login prompt from the target router.**

   The system displays the following prompt:

   ```
   Login:
   ```

6. **Enter Manager and a password, if necessary, to log in to the router's Technician Interface.**

   The system displays the following message and prompt:

   ```
   Welcome to the <Node_Type> Technician Interface.
   $
   ```

7. **Enter a cd command to designate the disk volume or memory card "volume" that should receive the files you want to transfer from your UNIX workstation.**

   For example:

   cd a: (designates diskette Volume a)

   or

   cd 2: (designates a memory card volume in router Slot 2)

8. **Enter the xmodem receive binary command, as follows:**

   xmodem rby

   rb is a receive binary file.

   y is the YMODEM file transfer option.

9. **Type ~c (tilde-c) to escape momentarily from the Technician Interface command line prompt to the UNIX workstation command line prompt.**

   The workstation responds

   ```
   Local command?
   ```

10. **Enter an xmodem send binary command with the print (display) transfer events and information option flag (p) set in the command line, as follows:**

    xmodem sbyp *<source_vol/dir>:<filename> . . .<filename>*

    sb is a send binary file.

    y is the YMODEM file transfer option.

    p prints (displays) important information and events pertaining to the file transfer(s) you are about to initiate.

    <*source_vol/dir*> = The disk drive volume and directory that contain the files you want to send to the router.

    <*filename*> . . .<*filename*> = The names of the files you want to send from the workstation to the router. If you want to enter multiple filenames as part of a YMODEM batch file transfer operation, insert a space character between filenames. (For more information on Technician Interface filename specifications, refer to Chapters 4 and 5.)

    Pressing return to execute the **xmodem** command triggers the necessary handshakes between the YMODEM protocol program running on the workstation and the YMODEM program running on the router. This handshaking in turn triggers the start of the file transfer(s) you specified in the **xmodem** command entered at the UNIX command line prompt.

Workstation and router response: (typical)

```
-----------------
XMODEM Send Function
File Name: atl.cfg
File Size: 7k, 56 Records, 7160 Bytes
Estimated transmission time 9 seconds
Receiver invoked CRC mode
Non-ACK on sector 1
Sector 0 sent
Sector 32 sent
Send Complete
56 Sectors Transferred in 31 seconds
Transfer Rate = 231 Characters per Second
Closing down Batch Transmission
Non-ACK on Sector 1
Sector 0 sent
Batch Send Complete
```

`away for 40 seconds` (the amount of time the workstation's command line relinquished control to the workstation's YMODEM protocol program; i.e., the duration of the file transfer operation)

```
!
$
```

11. **Enter the dir command to list the contents of the receiving volume in order to verify that the file transfer operation completed successfully.**
12. **If you are finished transferring files from the router to the workstation, enter logout.**

    This action returns control to the UNIX workstation command line prompt.

Out-of-Band File Transfers from a Windows Workstation

This section describes the Bay Networks Communications Terminal Program and its applications for logging in to the Technician Interface of a remote router and for transferring files to and from a router.

xmodem and the Bay Networks Communications Terminal Program

The Bay Networks Communications Terminal Program (filename *wfterm.exe*) is an ASCII terminal emulation utility included with your Site Manager (for Windows 3.1) PC software. Nearly identical in purpose to the **tip** (Terminal Interface Program) command on a UNIX workstation, *Wfterm* enables you to

- Dial in to the Technician Interface port of a router.
- Log in to the Technician Interface for that router (start a Technician Interface session).
- Initiate Technician Interface commands. (For out-of-band file transfers to and from a router, you run the **xmodem** commands described in the section "About xmodem.")
- Close the connection between the workstation and the router.

Before you use *Wfterm* and enter any **xmodem** command, you must

- Open *Wfterm* (from its icon in the Site Manager program group)
- Enter *Wfterm* setup information (local modem settings and the phone number of a target router)

Opening Wfterm

You can open *Wfterm* by double-clicking on its icon in the Site Manager icon group, as shown in Figure B-2.

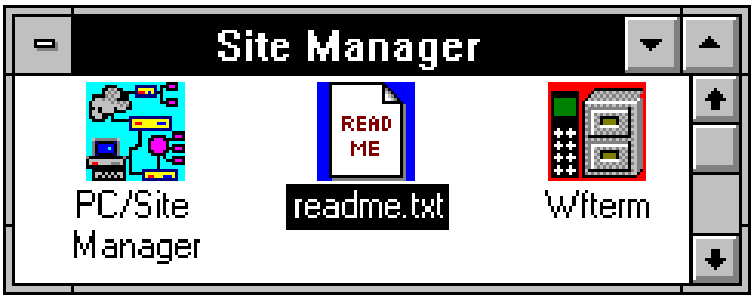


Figure B-2. Wfterm Icon

Wfterm opens the window shown in Figure B-3.

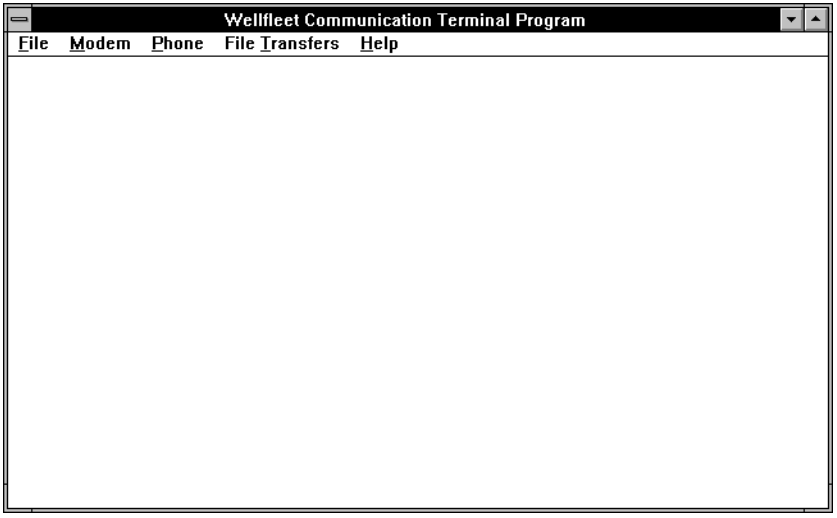


Figure B-3. The Wfterm Base Program Window

From this window, you can

- Check current settings or enter new settings for the interface to the modem locally attached to your workstation.
- Initialize the locally attached modem with the current settings.
- Enter a telephone number, initiate autodialing, and open a connection to a remote target router.
- Log in to the Technician Interface of the remote router.
- Transfer files between the router and your workstation. (You can initiate other Technician Interface commands as well at the Technician Interface prompt inside the *Wfterm* program window. However, this section does not provide information on Technician Interface procedures other than those required to support **xmodem** out-of-band file transfers.)
- Log off the target router (terminate the Technician Interface session).
- Disconnect/terminate the connection between the workstation and the target router.

If you are opening *Wfterm* for the first time, proceed to the next section, "Checking and Verifying Current Modem Interface Settings."

If you are sure that the current interface settings for the modem locally attached to your workstation are already correct, and you have determined the types of file transfer operations you need to perform, proceed to "Initializing the Local Modem."

Checking and Verifying Current Modem Interface Settings

You must ensure that the modem locally attached to your workstation can establish a connection with a modem attached to the Technician Interface port of a remote target router. To satisfy this requirement, you need to check current settings for the physical-layer interface to that modem. If the settings you observe are inappropriate for the type of data link and modem attached to the remote target router, you can enter new settings dynamically, through the Wfterm Communications Settings window. You access this window by selecting the Settings option of the Modem pull-down menu in the *Wfterm* startup window, as shown in Figure B-4. This menu selection invokes the window shown in Figure B-5.

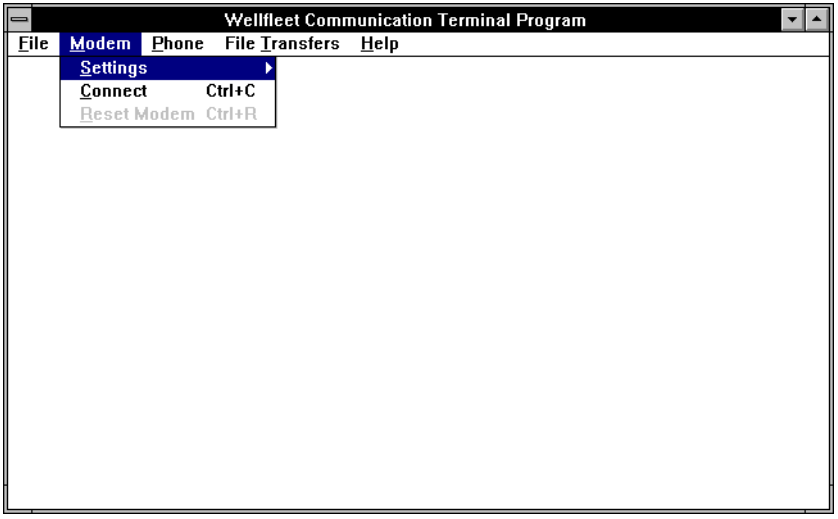


Figure B-4. Accessing the Modem Settings Window

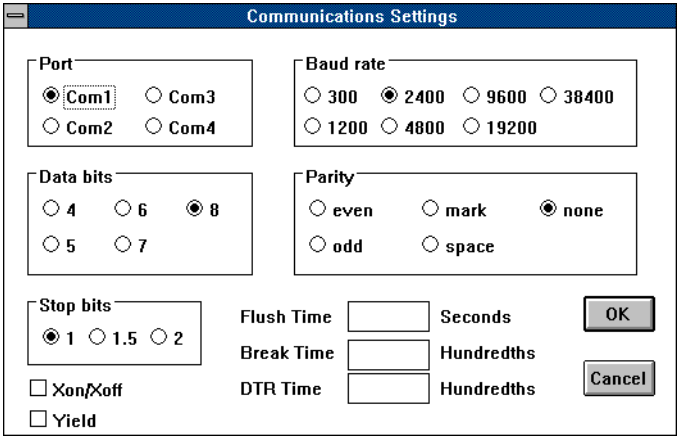


Figure B-5. Verifying or Modifying Modem Interface Settings

You access this window by means of the Modem/Settings pull-down menu in the *Wfterm* base program window.

The settings shown in Figure B-5 reflect default operational values for any Hayes compatible modem. However, if you are sure that current interface settings for the modem locally attached to your Site Manager workstation are correct, proceed to "Initializing the Local Modem."

If you are unsure of the current modem interface settings, refer to the user manual supplied with the modem, make the required changes to the modem interface settings, then proceed to the next section, "Initializing the Local Modem."

Initializing the Local Modem

Before attempting to open a dial connection between your workstation and a remote target router, you need to initialize and "wake up" the modem locally attached to the PC. You initialize the modem by selecting the Connect option of the *Wfterm* Modem pull-down menu. You verify that the local modem has initialized successfully when you observe and respond to the message window shown in Figure B-6.

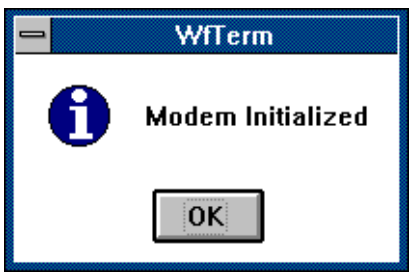


Figure B-6. Verifying Successful Modem Initialization

Use the cursor to press the OK button. The following message appears below the Modem Initialized window:

```
ATS0 = 0
OK
```

With the local modem online and initialized, you can access and use the telephone call functions supported by the *Wfterm* utility, as described in the next section, "Using Wfterm Telephone Call Functions."

Using Wfterm Telephone Call Functions

You can access two telephone call functions from the Phone pull-down menu of the *Wfterm* base program window, as shown in Figure B-7.

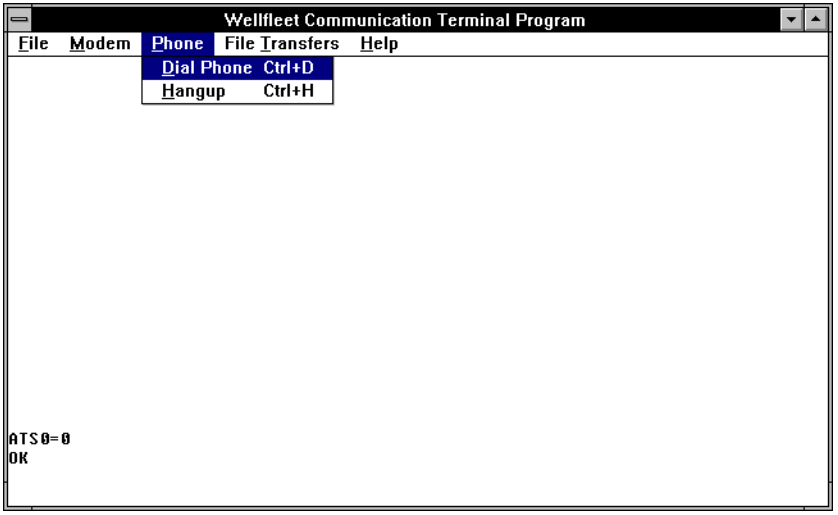


Figure B-7. Accessing Wfterm Telephone Call Functions

Dialing a Remote Router

To dial and connect to the Technician Interface port of a remote router, select the Dial Phone function of the *Wfterm* pull-down menu. The Dial Command window appears, as shown in Figure B-8.

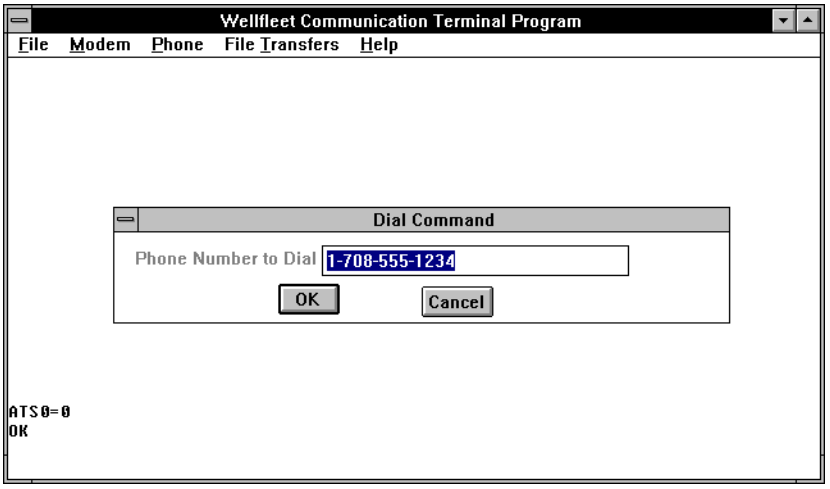


Figure B-8. The Wfterm Dial Command WIndow

Enter in the Dial Command window the telephone number of a router that has a configuration file you want to retrieve. Using the cursor to press the OK button initiates the dialing sequence.

Note: This release of the *Wfterm* utility allows you to enter and store one telephone number in the Dial Command window. Each time you need to call a different router, enter the telephone number of that router in the Dial Command window. It may be helpful for you to maintain a list of the telephone numbers for every router you need to access by means of out-of-band, dial-in connection.

The *Wfterm* utility always retains the last number you enter. Closing and reopening *Wfterm* does not clear the number last stored.

If the call in progress is successful, *Wfterm* opens a connection between your Site Manager workstation and the Technician Interface port of the called router. The Technician Interface login prompt appears in the *Wfterm* base program window, but you may have to press return to invoke the Technician Interface prompt.

If the call in progress is unsuccessful, *Wfterm* displays an appropriate message in the base program window.

Once *Wfterm* connects to the Technician Interface port of a router, you must log in to that Technician Interface.

Logging In to the Router's Technician Interface

Once *Wfterm* connects to the Technician Interface port of a router, log in to the router's Technician Interface as follows:

1. **Press return, if necessary, to invoke the Technician Interface login prompt from the target router. Watch for the prompt in the *Wfterm* base program window.**

   The system displays the following prompt:

   ```
   Login:
   ```

2. **At the login prompt, enter Manager.**

   The system displays the following message and prompt:

   ```
   Welcome to the <node_type> Technician Interface.
   $
   ```

Note: Your network administrator may have customized the Welcome message and login prompt for the router on which you are attempting a login procedure.

Once you are logged in to the router's Technician Interface, you can transfer files to and from that router.

File Transfer Functions

Once you are logged in to the router's Technician Interface, you can access and use the file transfer functions of the *Wfterm* utility by means of the File Transfers pull-down menu (Figure B-9).

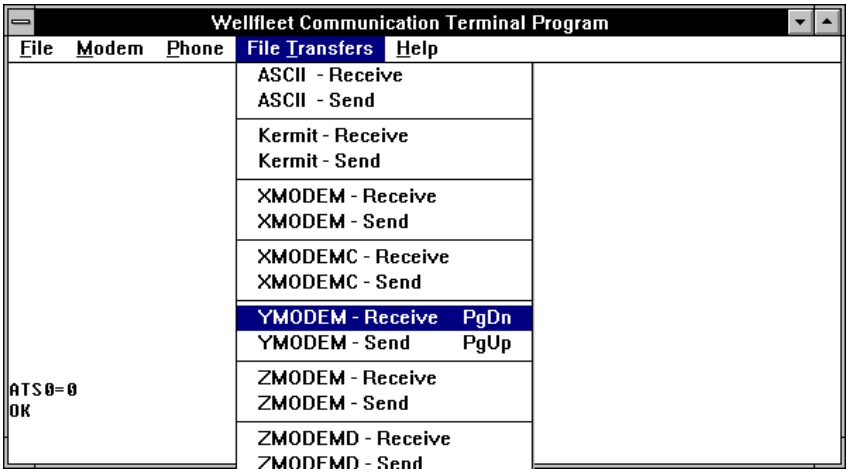


Figure B-9. The Wfterm File Transfer Operation Selection Window

Note: Because the *Wfterm* utility provides more functionality than is required to support YMODEM file transfers, the File Transfers pull-down menu contains options for up to fourteen different file transfer operations. However, to transfer files between a workstation and a Bay Networks router, you need only the **ymodem-send** and **-receive** options. This section provides only the information you need for the YMODEM options.

Transferring Files from Router to DOS Workstation

To transfer one or more files from a router to your Site Manager workstation, you must

- Be logged in to the Technician Interface of the desired router. (Refer to the earlier section, "Logging In to the Router's Technician Interface.")
- Select the disk volume or memory card "volume" that contains the files you want to transfer to your workstation.
- Set the receiving *Wfterm* utility into receive mode.
- Trigger or initiate the file transfer from router to workstation.

Proceed as follows to transfer one or more files from router to workstation:

1. **Enter a cd command to designate the disk volume or memory card "volume" that contains the files you want to transfer to your UNIX workstation.**

   For example:

   cd a: (designates diskette Volume a)

   or

   cd 2: (designates a memory card volume in router Slot 2)

2. **Enter a dir command to view the list of files in the volume/memory card.**

   The system displays a screen similar to the following table:

File Name	Size	Date	Day	Time
abc.cfg	1814	10/28/94	Thurs.	10:29:06
def.cfg	2293	11/03/94	Wed.	17:16:29
ghi.cfg	4197	11/15/94	Mon.	08:34:04

3. **Determine which files you need to transfer from the router to the workstation.**

4. **Enter the xmodem send binary command, as follows:**

   xmodem sby *<source_vol>*:*<filename>*

   sb is a send binary file.

   y is the YMODEM file transfer option.

   <source_vol> is either a slot number of a memory card or the letter of the disk drive volume that contains the files you want to send to the workstation.

   <filename> is the name of the file you want to send from the router to the workstation. If you want to enter multiple filenames as part of a YMODEM batch file transfer operation, insert a space character between the filenames. (For more information on Technician Interface filename specifications, refer to Chapters 4 and 5.)

Note: To ensure that files are transferred properly, do not issue the **xmodem** command with the <wait> parameter when you perform out-of-band file transfers to or from a Windows workstation that has Wfterm running on it.

5. **To set the receiving *Wfterm* utility into receive mode, select the YMODEM-Receive option from the File Transfers pull-down menu.**

   Selecting this option invokes the File to Transfer window, as shown in Figure B-10.

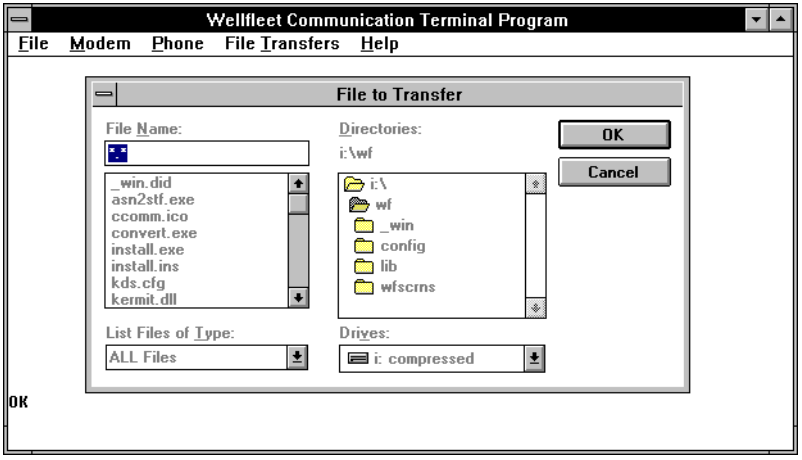


Figure B-10. The Wfterm File to Transfer Window

6. **Select/highlight the drive and directory that should receive the file from the router.**

   If you want to rename the file upon receipt at the workstation, you can also type a filename into the File Name line of the File to Transfer window.

7. **Use the cursor to press the OK button in the File to Transfer window.**

   Pressing the OK button notifies the sending Technician Interface to terminate its wait-before-transmit state, and to send the file you specified in the File to Transfer window.

8. **You verify that the file transfer was successful when you see the File Transfer Completed message in the *Wfterm* base program window.**

   You should also see the filename appear in the receiving directory on the workstation. If the transfer was unsuccessful, you should see the message

   ```
   File Transfer Aborted.
   ```

9. **If you are finished transferring files from the router to the Site Manager workstation, enter logout at the Technician Interface command line prompt in the *Wfterm* base program window.**

At the conclusion of file transfer operations, you can close the connection between the workstation and the router. (Refer to the later section, "Closing the Connection.")

Transferring Files from DOS Workstation to Router

To transfer one or more files from your Site Manager workstation to a router, you must

- Log in to the Technician Interface of the desired router. (Refer if necessary to the earlier section, "Logging In to the Router's Technician Interface.")
- Select the disk volume or memory card "volume" that should receive the file you want to transfer from your workstation.
- Set the receiving Technician Interface into binary receive mode.
- Set the sending *Wfterm* utility into binary send mode.
- Select the disk volume, directory, and file you want to send to the router.
- Trigger or initiate the file transfer from workstation to router.

Proceed as follows to transfer one or more files from workstation to router:

1. **At the Technician Interface command line prompt, enter a cd command to designate the disk volume or memory card "volume" that should receive the desired file from the workstation.**

   For example:

   cd a: (designates diskette Volume a)

   or

   cd 2: (designates a memory card volume in router Slot 2)

2. **At the Technician Interface command line prompt, enter the xmodem receive binary command, as follows:**

   xmodem rbye

   rb is a receive binary file.

   y is the YMODEM file transfer option.

   e disables the EOT verification.

Note: To ensure that files are transferred properly, do not issue the **xmodem** command with the <wait> parameter when you perform out-of-band file transfers to or from a Windows workstation that has *Wfterm* running on it.

3. **Set the sending *Wfterm* utility into send mode by selecting the YMODEM-Send option from the File Transfers pull-down menu.**

   Selecting this option invokes the File to Transfer window, as shown in Figure B-10.

4. **Select/highlight the drive, directory, and file you want to send to the router.**

5. **Use the cursor to press the OK button in the File to Transfer window.**

   Pressing the OK button initiates the file transfer to the router.

6. **You verify that the file transfer was successful when you see the** File Transfer Completed **message in the *Wfterm* base program window.**

   If the transfer was unsuccessful, you should see the message File Transfer Aborted.

7. **You can optionally enter a dir command at the Technician Interface command line prompt in order to verify that the file you sent now exists in the router disk or memory card volume you set in Step 4.**

8. **If you are finished transferring files from the workstation to the router, enter logout at the Technician Interface command line prompt in the *Wfterm* base program window.**

At the conclusion of file transfer operations, you can close the connection between the workstation and the router. (Refer to "Closing the Connection.")

Closing the Connection

You can “gracefully” close the connection between your workstation and a target router after you

- Finish transferring (downloading or uploading) files between the remote router and your workstation
- Log off the Technician Interface of the target router

To close a connection, select the Hangup function in the *Wfterm* File pull-down menu, as shown in Figure B-7. When the connection closes, the Wfterm Connection Closed window appears, as shown in Figure B-11.

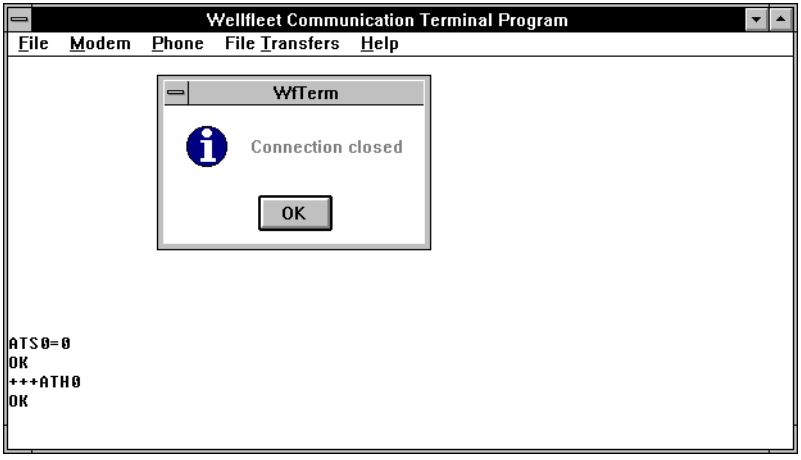


Figure B-11. The Wfterm Connection Closed Window

At any time you can also close a connection simply by quitting the *Wfterm* utility. Once you close the connection between your workstation and the target router, you can quit the *Wfterm* program, as described in the next section.

Quitting Wfterm

You can quit the *Wfterm* utility after you

- Finish transferring files
- Log out of the Technician Interface of the target router
- Close the connection between your workstation and the target router

Quit *Wfterm* by selecting the Exit option under the File pull-down menu, as shown in Figure B-12.

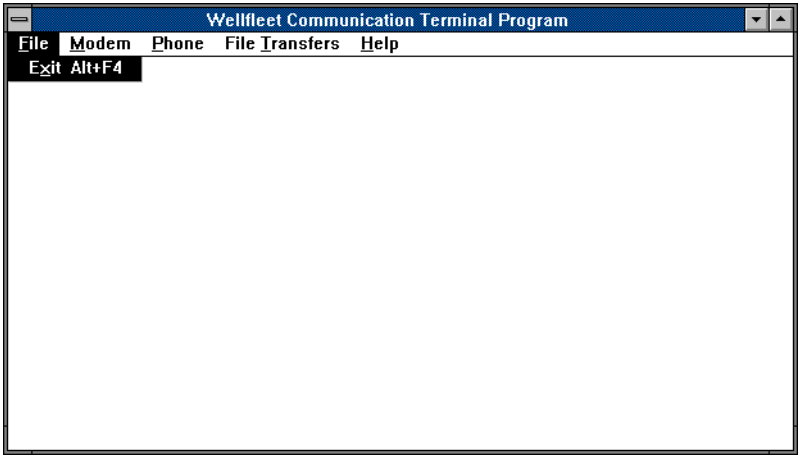


Figure B-12. Exiting/Quitting the Wfterm Program

Appendix C
Using Syslog Messaging to Monitor Router Events

This appendix provides

- An overview of Syslog services on a Bay Networks router and counterpart Syslogd services on a UNIX workstation
- Procedures for
  - -- Configuring Syslogd on a UNIX workstation
  - -- Configuring Syslog services on a router
  - -- Managing Syslog services on a router
- An example Syslog configuration
- Descriptions of Syslog MIB attributes (parameters)

To use the information in this appendix, you should have experience with UNIX system commands and facilities, and also with the Technician Interface for Bay Networks routers.

Overview

You can use the *Syslog* messaging feature of the Bay Networks router software to manage router event messages on any UNIX-based network management platform. The Syslog software supports this functionality by communicating with a counterpart software component named *Syslogd* on your management workstation.

Syslogd is a UNIX daemon software component that receives and locally logs, displays, prints, and/or forwards messages that originate from sources internal and external to the workstation. For example, Syslogd on a UNIX workstation concurrently handles messages received from applications running on the workstation, as well as messages received from Bay Networks routers running in a network accessible to the workstation.

Figure C-1 illustrates the following Syslog and Syslogd functionality:

Syslog running on each slot

- Polls the local events log buffer to retrieve new event messages.
- Selects from the local events log messages that meet the requirements of entity filters you configure on the router.
- Maps into Syslog message format any messages retrieved from the local events log.
- Inserts a priority code into each reformatted message.
- Time-sequences messages if you first enabled the message sequencing feature.
- Forwards messages to IP on the router, which in turn forwards messages to remote hosts identified in the Syslog host table.

At a remote UNIX management workstation, Syslogd

- Receives Syslog messages from Bay Networks routers.
- Examines the priority code in each message.
- Uses the priority code to determine appropriate system handling for each message.
- Based on the priority code in each message, Syslog dispatches each message to any or all of the following destinations:
  - -- Workstation display
  - -- A local log file
  - -- A designated printer
  - -- One or more remote hosts

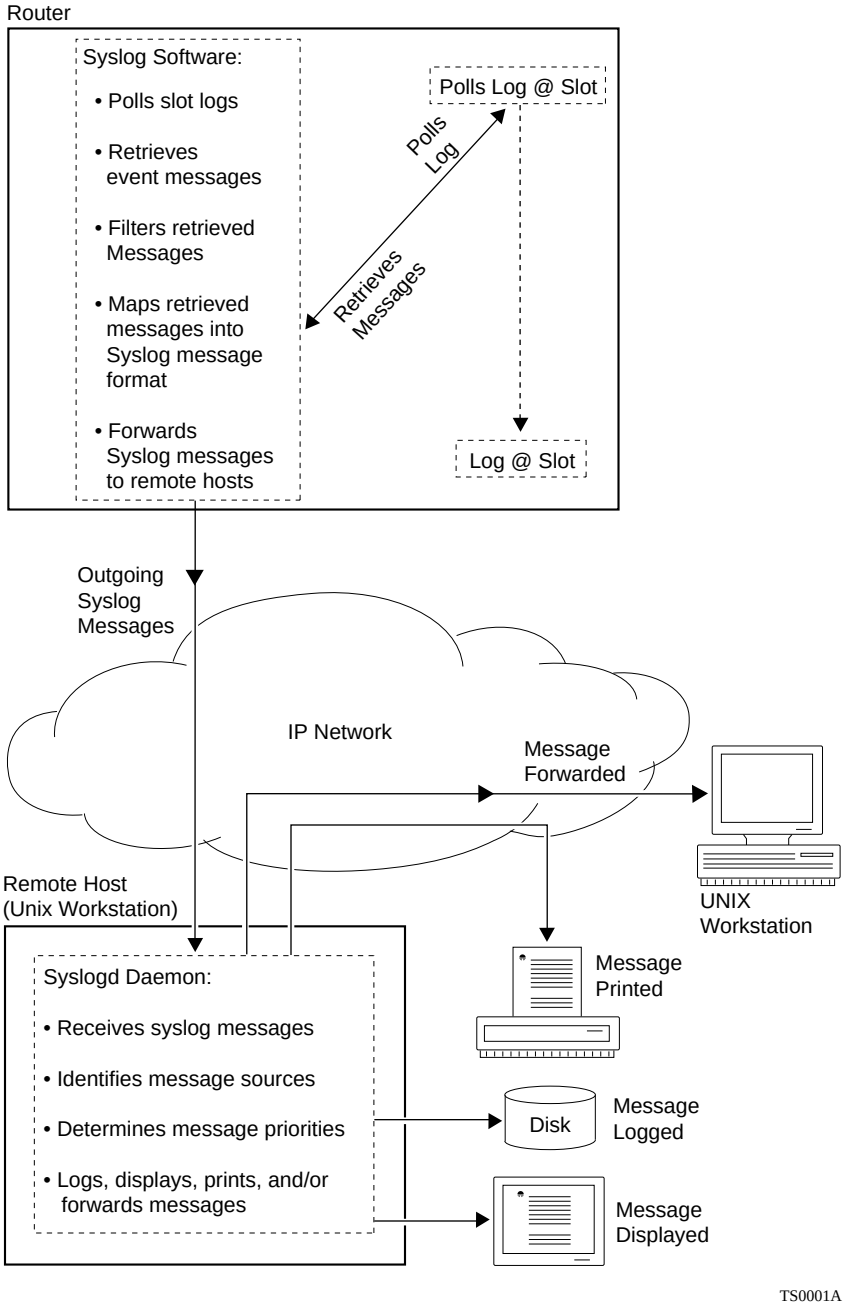


Figure C-1. Syslog and Syslogd Operation

Remote Hosts and Filters

You use a management workstation to monitor event messages generated by specific software entities on each router in your network. To receive at a management workstation event messages from a router, you must

- Enable Syslog on the router.
- Define in the Syslog host table any remote hosts you want to receive messages.
- Configure entity-specific message filters for each host.

You can configure entity filters by means of the Configuration Manager tool under Site Manager, or by means of **set** and **commit** commands you enter at the Technician Interface of the router.

Note: This appendix covers Syslog configuration via Technician Interface commands only. (For information on how to configure Syslog through Site Manager, refer to *Managing Routers and BNX Platforms*.)

Each entity filter selects only event messages that

- Originate from a router software entity that you specify by entity number AND
- Have an event message number OR severity level that matches one of the values you configured AND
- Originate from a router slot you specify

Figure C-2 illustrates how an entity filter limits the number of event messages forwarded by Syslog from a router to a specific remote host. Each filter attribute or parameter (entity number, event numbers or severity levels, and slot numbers) that you specify increases the selectivity of a filter.

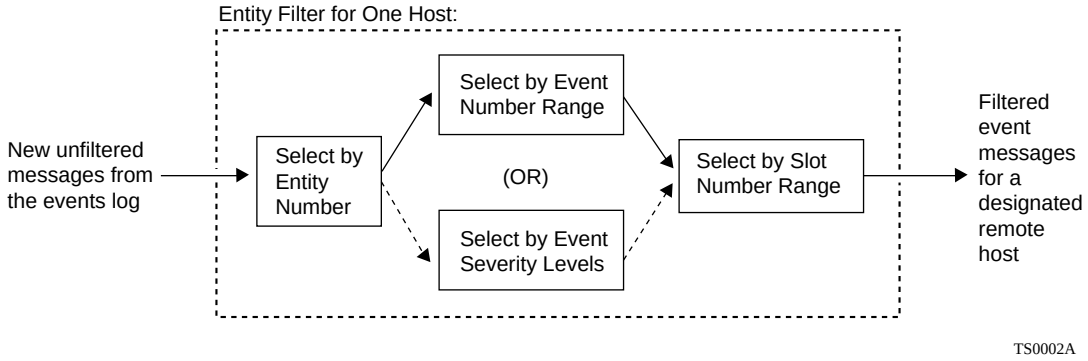

Entity Filter for One Host:
New unfiltered messages from the events log
Select by Entity Number
Select by Event Number Range
(OR)
Select by Event Severity Levels
Select by Slot Number Range
Filtered event messages for a designated remote host
TS0002A

Figure C-2. Router Event Message Filtering for One Host

Polling the Events Log

Syslog polls the events log buffer on the local slot to retrieve any new messages logged since the previous polling attempt. Syslog polls the local slot at an interval determined by the set value of the wfSyslogPollTimer (poll timer) attribute. You can accept the system default value or set a customized value for this attribute.

Identifying Entity Filters

Each protocol and system service in the router software has a unique entity number. (For a complete list of entity numbers, refer to the guide *Event Messages for Routers and BNX Platforms*.) The router software uses an entity number plus the IP address of a specific remote host to identify each entity filter you configure on the router.

For example, if you configure a filter that selects only messages logged by entity number 2 (IP) on a router, Syslog forwards those messages only to the host IP address associated with that filter.

You must also assign a *filter index* number (wfSyslogEntFltrIndex) to each filter you configure for the same entity and remote host pair. Assign a value of 1 to the first filter you configure for a specific entity and remote host pair. To each subsequent filter that you configure for the same entity and remote host pair, assign an index number, increased by +1.

Note: Although you assign each filter an index number manually through the Technician Interface, Site Manager automatically assigns an index number to each new filter you add to the configuration.

When you want Syslog to select and forward from *all entities* event messages that satisfy severity and slot criteria that you specify, configure a filter for the *wildcard entity number* (255).

Note: The wildcard filter is active for a host, only if there are no other entity filters active for that host. If you configure and activate a filter for any entity number other than 255, that filter takes precedence over the wildcard filter. The wildcard filter transitions to the inactive state. The setting of the attribute wfSyslogEntFltrOperState indicates the current operational state of any filter instance you configure for a given host. (If wfSyslogEntFltrOperState = 1, the filter is active; if wfSyslogEntFltrOperState = 2, the filter is inactive.)

Filtering by Event Number

Each event message generated by the router software has a unique message number. (For a complete list of event message numbers, refer to the guide *Event Messages for Routers and BNX Platforms*.)

You can use event message numbers to specify an entity filter that selects only the types of messages you want a remote host to receive.

You define a range of event message numbers for a router software entity by specifying

- An upper boundary number (MIB object wfSyslogFltrLogEvtUppBnd)
- A lower boundary number (MIB object wfSyslogFltrLogEvtLowBnd)

Syslog considers the upper and lower boundary values as part of the range.

For example, an entity filter for FTP has an Event Number Range with a lower boundary of 5 and an upper boundary of 27. With this filter, Syslog forwards to a remote host FTP log messages with event numbers 5 to 27, inclusive.

You can specify a filter for an individual message by setting the upper and lower boundaries of the event number range equal to the same message number.

If you configure an event number range of 0 to 255, *Syslog ignores the range as a filtering parameter* and checks instead to see if a Message Severity Mask exists for the same entity filter.

Filtering by Event Severity Level

Each event message generated by the router software has a unique severity level. (To determine the severity level of any router event message, refer to the guide *Event Messages for Routers and BNX Platforms*.)

As an alternative to specifying event numbers as filtering criteria, you can specify in an entity filter one or more event message severity levels (that is, you define a severity mask for the filter).

Note: Syslog checks the message severity mask only when you accept the default event message number range of 0 to 255 for the same filter. This causes Syslog to ignore event numbers as criteria for selecting and forwarding messages to a remote host.

Syslog uses the severity levels as criteria for selecting and forwarding only the types of messages you want a remote host to receive.

An entity filter passes only messages that have a severity level equal to any you specified in the message severity mask. You define severity levels by setting a value for the wfSyslogEntFltrSevMask filter attribute in the router's active MIB.

For example, if an entity filter for FTP has a Message Severity Mask of "wfi," the filter passes only FTP event messages that have a severity level of warning (w), fault (f), or information (i).

Filtering by Slot Number

The router stores event messages in the log buffer associated with each slot. You can configure an entity filter to select for forwarding only event messages logged on the slots you specify. (You must specify at least one slot in the range 1 to 14, where the slot numbers depend on the model of router.)

You define a range of slot numbers for an entity filter by specifying

- An upper boundary number (MIB object wfSyslogFltrSlotUppBnd)
- A lower boundary number (MIB object wfSyslogFltrSlotLowBnd)

Syslog considers the upper and lower boundary numbers as part of the range. For example, you can configure an entity filter for FTP with an event number range of 5 to 27 and a slot number range of 2 to 5. In this case, Syslog forwards to the associated remote host FTP log messages numbered 5 to 27 logged on Slots 2 to 5 only.

You can configure a filter to select messages logged on a specific slot by setting the upper and lower slot boundary values to the same number.

Note: With both the upper and lower boundary attributes set to 0 (the default value for those attributes), the filter cannot transition to the active state.

Mapping Router Event Messages into Syslog Message Format

Syslog running on each slot maps filtered event messages into Syslog message format. For example, the following system log message

```
#1: 02/07/95 16:03:18.679 INFO SLOT2  FTP  Code:5
FTP is initializing.
```

looks as follows in Syslog format:

```
<AE>FTP: SLOT:2 SEVERITY:Info ENTITY_CODE/EVENT_CODE:88/5
FTP is initializing.
```

Figure C-3 shows how Syslog encapsulates a message into a UDP packet.

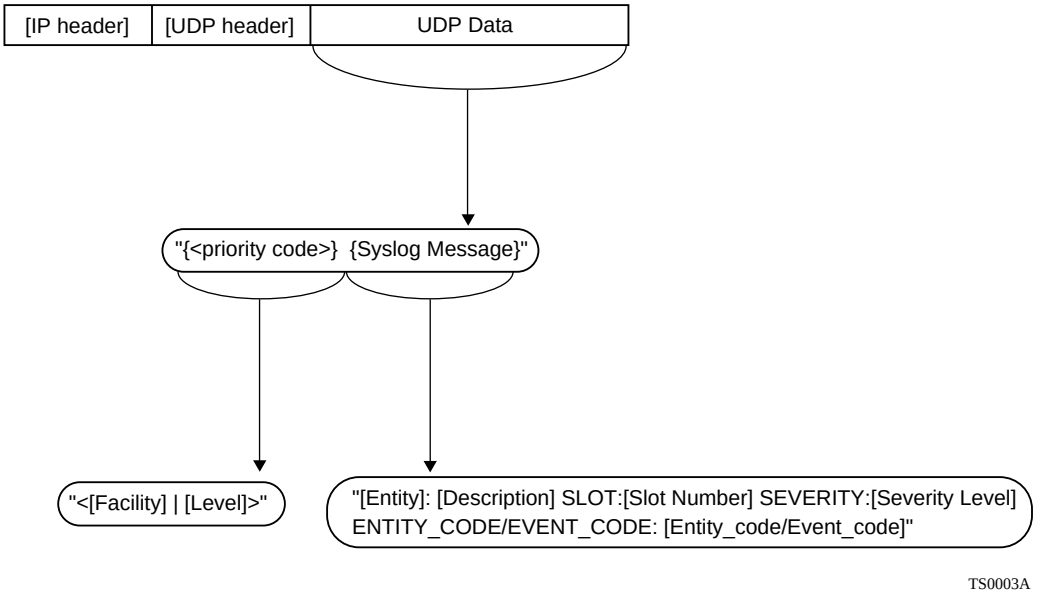


Figure C-3. Syslog Message Encapsulation

Syslog retrieves the variables shown in brackets ([ ]) from the router's system log message or from the host table. The following paragraphs describe the variables for

- IP header
- UDP header
- UDP data
- Priority code

IP Header

Syslog adds to any event message that passes all filtering criteria the destination IP address for a specific remote host.

UDP Header

Syslog adds to any event message that passes all filtering criteria the destination UDP port number on the remote host identified in the IP header.

UDP Data

The UDP data field in the Syslog packet contains a reformatted router event message, plus a priority code required by the remote host. The remote host uses this information to make decisions on how to handle messages received from a router.

Priority Code

The example of a priority code and its text (Figure C-4) consists of a *facility code* plus an *error level code* (in the form *facility.error*).

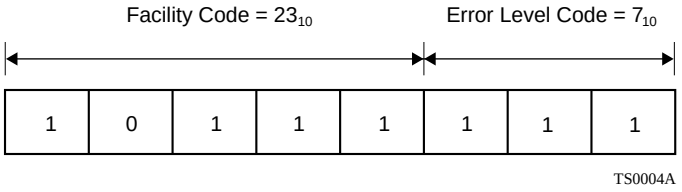


Figure C-4. Syslog Message Composition

The facility code identifies a standard UNIX system facility that receives a message from an internal or external software entity. The “Local <0-7>” UNIX system facilities receive event messages (in Syslog format) from routers in your network. The following table relates UNIX system facility names to their respective facility codes on a workstation.

UNIX System Facility Name	Facility Code (equivalent decimal value)
Local 0	1
Local 1	2
Local 2	3
Local 3	4
Local 4	5
Local 5	6
Local 6	7
Local 7	8

The error level code identifies the severity level (level of urgency) of a received message for UNIX system handling decisions (such as logging, displaying, printing, or forwarding the message). The following table shows one way to map UNIX system error codes and error levels to the severity levels of event messages from Bay Networks routers.

UNIX System Error Codes	UNIX System Error Levels	Suggested Mapping to Bay Networks Router Event Message Severity Levels
1	LOG_EMERG	Fault
2	LOG_ALERT	Warning
3	LOG_CRIT	Warning
4	LOG_ERR	Warning
5	LOG_WARNING	Warning
6	LOG_NOTICE	Info
7	LOG_INFO	Info
8	LOG_DEBUG	Debug, Trace

You determine how Bay Networks router event message severity levels map to error levels on your UNIX workstation, based on requirements of the network management application software you want to use.

Refer to "Configuring Syslog on the Router" for instructions on how to map router event messages to UNIX system facility and error level codes.

Time Sequencing Syslog Messages

If you enable the message time-sequencing feature, Syslog on each slot

- Polls that slot for event messages logged since the previous polling attempt
- Filters all event messages retrieved via polling
- Reformats router event messages into Syslog message format
- Forwards Syslog messages to a Sequencer gate, which arranges in time-stamp order any messages it receives
- Forwards sequenced messages from the router to the appropriate remote hosts

Without sequencing, Syslog polls, filters, reformats, and forwards messages from each slot to IP on the router. IP forwards the messages in retrieved order to the appropriate remote hosts.

Syslog Message Handling (on a Workstation)

Syslogd on your management workstation uses the priority code in each locally received Syslog message to

- Determine that the message came from an external source (a Bay Networks router in an IP network accessible to the workstation), rather than from an internal source (such as the workstation's email system or line printer spooling system)
- Determine whether to redispatch the message to a local log file, to the workstation display, to a printer, or to another remote UNIX host

Syslogd makes these determinations by examining the two parts of the priority code (*facility.error*) in each message.

Refer to “Configuring Syslog on the Router” for instructions on how to enable the Syslog time sequencing feature.

Note: Enable time sequencing only when it’s important for your management workstation to receive router event messages in time-stamped order, rather than in order of retrieval from each slot. (When you enable the time-sequencing feature, Syslog requires more processing resources from the router.)

Configuring Syslogd on a UNIX Workstation

Before you configure and activate Syslog on any routers, configure Syslogd on UNIX network management workstations in your network. This helps to prevent the loss of event messages you may want to capture as you begin to enable Syslog on each router.

UNIX workstations have a *syslog.conf* file in which you define destinations for event messages received by the local Syslogd software module. For Syslogd to properly dispatch router event messages to a file, display, printer, and/or another remote host, you must edit the contents of the */etc/syslog.conf* file.

Configure Syslogd on your UNIX workstation, as follows:

1. **Log in as superuser, as follows:**

   su root

2. **Open** */etc/syslog.conf* **and examine the** <*facility.level*> **indicators,** **local**<*0 - 7*>**.**<*fault* | *warning* | *info* | *trace* | *debug*>**.**

3. **Edit** */etc/syslog.conf* **as needed to achieve message handling appropriate for your management workstation requirements.**

Example:

Messages dispatched to console display:

local7.debug	/dev/console
local7.info	/dev/console
local7.notice	/dev/console
local7.err	/dev/console
local7.crit	/dev/console
local7.alert	/dev/console
local7.emerg	/dev/console

or:

local7.debug;local7.info;local ;local7.notice;
local7.err;local7.crit;local7.alert;local7.emerg /dev/console

Messages dispatched to a file:

local7.info	/var/log/syslog.file
local7.debug	/dev/log/debug_file
local7.warning	/var/log/warning_file

Messages dispatched to a host:

local7.notice	@<*host_name*>

Messages dispatched to a printer:

local7.trace	@<*printer_name*>

In this example, the path specified next to each “local” facility indicator in the file shows a unique destination for each severity level of router event message.

4. **Save the changes you made to** *syslog.conf***.**
5. **Enter the UNIX ps command to obtain the process id for the Syslogd process currently running on the workstation.**
6. **Reinitialize Syslogd by entering the following command at the UNIX command line prompt:**

   kill -HUP *<process_id>*

Configure in the same way any other UNIX workstations you use to manage your network.

To *view* on a UNIX workstation event messages from a Bay Networks router, open the file you designated on the workstation to receive Syslog messages from routers in your network.

Configuring Syslog on the Router

You can use Technician Interface commands to configure Syslog on a router. You configure Syslog as a sequence of *tasks*, where some tasks include one or more numbered *steps*.

The following is an overview of the tasks required to configure Syslog on a router:

1. Using the console attached to the router, or using a Telnet connection to the router, open a Technician Interface session.
2. Define a slot mask (a slot map) for loading Syslog on the router.
3. Create the Syslog entity on the router.
4. Configure Syslog global attributes.
5. Add a remote host to the Syslog Host Table.
6. Add an entity filter to the Syslog entity filter table.
7. Return to Task 5 to add another remote host or return to task 6 to add another entity filter for the remote host; otherwise go to Task 8.
8. Save to a file on an NVFS volume the Syslog additions to your configuration.
9. Log out of the Technician Interface session.

The paragraphs following in this section describe the Syslog configuration sequence in greater detail (to the task *and* step level).

Following the configuration procedure, this appendix provides an example of Syslog configuration, plus definitions of Syslog attributes you use during configuration.

Task 1: Logging In to the Router's Technician Interface

For information on how to open a Technician Interface session with a Bay Networks router, refer to Chapter 1.

Task 2: Defining a Slot Mask for Syslog on the Router

Before creating the Syslog entity on the router, define a slot mask for Syslog. The slot mask identifies the slots on which the system will load and run the Syslog entity. At the Technician Interface prompt, enter

```
$: set wfProtocols.wfSYSLLoad.0 0x7FFE0000;commit
```

This command enables Syslog to run on all slots, regardless of router model.

Next, create the Syslog entity on the router.

Task 3: Creating Syslog on the Router

Create the Syslog entity in the router configuration, as follows:

```
set wfSyslog.wfSyslogDelete.0 1;commit
```

This also *enables* Syslog on the router. (The system sets the attribute wfSyslogDisable, OID = 1.3.6.1.4.1.18.3.3.2.15.1.2, in the Syslog base record to a value of 1.)

Next, configure the Syslog global attributes.

Task 4: Configuring Syslog Global Attributes

Once you create and enable Syslog on the router, you can accept the default values for the wfSyslogMaxHosts and wfSyslogPollTimer attributes, or you can configure a customized value for either attribute. If you want to accept default values for the Syslog global attributes, go to Task 5; otherwise, perform the following steps:

1. **Configure the maximum number of active hosts served by Syslog on the router:**

   $: set wfSyslog.wfSyslogMaxHosts.0 *<1 - 10>***;commit**

   The default setting for wfSyslogMaxHosts is 5 hosts. You can add to the Syslog Host Table more entries than the configured maximum, but Syslog forwards messages only to the first "*n*" *active* hosts, where *n* = the current value of wfSyslogMaxHosts.

2. **Configure the interval (in seconds) between Syslog polling cycles on the router:**

   $: set wfSyslog.wfSyslogPollTimer.0 *<5 - 610000>***;commit**

   The default setting for wfSyslogPollTimer is 5 seconds.

Next, add a remote host to the Syslog Host Table.

Task 5: Adding a Remote Host to the Syslog Host Table

You must define any remote hosts that you want to receive Syslog (event) messages from routers in your network.

If this is the first host you are adding to the Syslog host table, go to Step 1. Otherwise, you may want to first obtain a list of hosts already configured on the router. To list existing entries in the Syslog host table, enter the following command at the Technician Interface prompt:

list -i wfSyslogHostEntry

The list includes the instance IDs (in this case, the IP addresses) of all remote hosts currently defined in the Syslog host table.

1. **Add a new host entry to the Syslog Host Table, as follows:**

   $: set wfSyslogHostTable.wfSyslogHostDelete.*<host_IP_address>* **1**

   $: commit

   This entry informs Syslog of a remote host at the destination IP address that you specified.

   If you want to accept the default settings for host attributes wfSyslogHostLogFacility (184 = Local7) and wfSyslogHostTimeSeqEnable (2 = disabled), go to Task 6. Otherwise, continue with Step 2 to configure a customized setting for either attribute.

2. **To define the UNIX system facility you want to receive Syslog messages from the router, enter the following:**

   $: set wfSyslogHostTable.wfSyslogHostLogFacility.*<host_IP_address>* *<128|136|144|152|160|168|176|184>***;commit**

128 = local0	160 = local4
136 = local1	168 = local5
144 = local2	176 = local6
152 = local3	184 = local7

3. **To optionally enable Syslog message time sequencing for the remote host, enter the following:**

   $: set wfSyslogHostTable.wfSyslogHostTImeSeqEnable. *<host_IP_address>* **1;commit**

Note: Only hosts represented by entries that are ENABLED (wfSyslogHostDisable =1) and have an operational state of ACTIVE (wfSyslogHostOperState = 1) receive messages from Syslog on the router.

Next, add an entity filter for the host entry you just added.

Task 6: Adding an Entity Filter for a Remote Host

Once you define a host in the Syslog host table, add (define) an entity-specific message filter for the host.

If this is not the first filter for a given entity and remote host pair, first obtain a list of filter instances, as follows:

list -i wfSyslogEntFltrEntry

From the resulting list of instance IDs (of the form <*host_IP_address*>.<*entity_code*>.<*filter_index*>), determine the next <*filter_index*> number available to assign to a new filter, for a given <*host_IP_address*>.<*entity_code*> pair. The number you assign to the new filter will have a value of +1 higher than the highest <*filter_index*> in the list.

Now proceed to Step 1.

1. **Create a new filter for the desired entity and remote host pair by first creating an entry in the Syslog Entity Filter Table, as follows:**

   $: set WfSyslogEntityFilterTable.WfSyslogEntFltrDelete.
   <host_IP_address>.<entity_code>.<filter_index> **1;commit**

   <host_IP_address> is the IP address of the desired remote host (a management workstation).

   <entity_code> identifies the software entity for which you want Syslog to forward event messages to the remote host at the *<host_IP_address>*.

   <filter_index> is the next available index number you can assign to a filter for the desired entity and remote host pair.

2. **After you create an entity filter for a specific host, define**

   - An event number (or range) and a slot number (or range)

     or:

   - A severity mask and a slot number (or range)

Note: The filter remains inactive until you define the event and slot number(s), or the severity mask and slot number(s).

Set entity filter attributes, as follows:

a. **To define by event number(s) the event messages you want Syslog to select and forward to a specific remote host:**

   $: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtLowBnd.
   <host_IP_address>.<entity_code>.<filter_index> <0 - 255>

   $: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtUppBnd.
   <host_IP_address>.<entity_code>.<filter_index> <0 - 255>

   $: commit

   If you do not want to define filtering by event number(s), accept the default values for event number lower bound (0) and upper bound (255). (Go to Step 2b.) Accepting these default values causes Syslog to use only the severity and slot mask criteria for selecting and forwarding messages.

b. **Define a severity mask *only* if you did not already define an event number (or event number range). If you defined an event number or number range, Syslog ignores any severity mask for this filter.**

To define by severity levels the event messages you want Syslog to select and forward to a specific remote host, enter the following:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSevMask.
<host_IP_address>.<entity_code>.<filter_index> **"***<fwitd>"*

$: commit

c. To also define by slot number(s) the event messages you want Syslog to select and forward to a specific remote host, enter the following:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowUpp.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>

$: commit

Note: Although the valid range for the slot lower and upper boundaries is 0 to 14, specify only values within the range of actual slot numbers for the model of router you are configuring. Otherwise, the filter will not transition to an active state.

---

3. Define how router event message severity levels and UNIX system error levels map to one another.

In most cases, you accept the default mapping and go to Task 7. Otherwise, continue with the following instructions to customize the message mapping.

Enter at the Technician Interface prompt the command line(s) appropriate for the message mapping(s) you want to change:

a. Change router FAULT message mapping, as follows:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrFaultMap.
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>

The default value of wfSyslogEntFltrFaultMap is 3, mapping router FAULT level messages to UNIX system level CRIT messages.

b. Change router WARNING message mapping, as follows:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap.
<host_IP_address>.<entity_code>.<filter_index> *<1 - 8>*

The default value of wfSyslogEntFltrWarningMap is 5, mapping router WARNING level messages to UNIX system level WARNING messages.

Example:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap 5

The example command maps each Warning level router event message to a Warning level UNIX system error message

c. Change router INFO message mapping, as follows:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrInfoMap.
<host_IP_address>.<entity_code>.<filter_index> *<1 - 8>*

The default value of wfSyslogEntFltrInfoMap is 7, mapping router INFO level messages to UNIX system level INFO messages.

d. Change router TRACE message mapping, as follows:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrTraceMap.
<host_IP_address>.<entity_code>.<filter_index> *<1 - 8>*

The default value of wfSyslogEntFltrTraceMap is 3, mapping router TRACE level messages to UNIX system level CRIT messages.

e. Change router DEBUG message mapping, as follows:

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrDebugMap.
<host_IP_address>.<entity_code>.<filter_index> *<1 - 8>*

The default value of wfSyslogEntFltrDebugMap is 8, mapping router DEBUG level messages to UNIX system level DEBUG messages.

Task 7: Adding More Hosts or Entity Filters

You can add more hosts or entity filters to your Syslog configuration, as follows:

1. **If you have finished adding entity filters for this remote host, and you do not want to add another remote host at this time, go to Task 8. Otherwise, continue with Step 2.**
2. **If you want to add another entity filter for the same remote host, return to "Adding an Entity Filter for a Remote Host." Otherwise, continue with Step 3.**
3. **If you want to add another remote host to receive Syslog messages from the router, return to "Adding a Remote Host to the Syslog Host Table."**

Task 8: Saving Your Syslog Configuration on the Router

Save to a file on an NVFS volume the Syslog additions to your configuration, as follows:

save config *<vol>*:*<filename>*

Task 9. Log Out of the Technician Interface

Enter at the Technician Interface command line interface the following command:

$: logout

For more information on how to close a Technician Interface session with a Bay Networks router, refer to Chapter 1.

Managing Syslog on a Router

Once you finish configuring Syslog on a router, you may occasionally need to

- Disable or re-enable the entire Syslog entity on the router. (Refer in this section to "Disabling or Re-enabling Syslog on the Router.")
- Disable or re-enable a Syslog host or filter on the router. (Refer in this section to "Disabling or Re-enabling Syslog Hosts or Filters.")
- Delete remote hosts or entity filters from the current Syslog configuration. (Refer in this section to "Deleting Remote Hosts or Entity Filters from the Syslog Configuration.")
- Delete Syslog from the router. (Refer in this section to "Deleting Syslog from the Router.")

Disabling or Re-enabling Syslog on the Router

You can, if necessary, disable the Syslog service anytime after enabling it on a router. Enter the following command line to disable Syslog:

```
$:  set wfSyslog.wfSyslogDisable.0 2;commit
```

Disabling Syslog on the router

- Transitions all Syslog hosts and their filters to an INACTIVE operational state in the router configuration
- Halts all message forwarding from Syslog to any Syslog hosts configured on the router

You can also re-enable Syslog after disabling it on a router. Enter the following command line to re-enable Syslog:

```
$:  set wfSyslog.wfSyslogDisable.0 1;commit
```

Re-enabling Syslog on the router

- Transitions Syslog hosts and their filters to an ACTIVE operational state in the router configuration. (Only *n* Syslog host entries transition to the ACTIVE state, where *n* = the value of wfSyslogMaxHosts.)
- Resumes all message forwarding from Syslog to Syslog hosts configured on the router. (Syslog forwards messages to *n* hosts only, where *n* = the value of wfSyslogMaxHosts.)

Disabling or Re-enabling Syslog Hosts or Filters

You can disable or re-enable host or filter entries already defined in your Syslog configuration as follows:

1. **Disable or re-enable message forwarding to a Syslog host, as follows:**

   a. **Disable a Syslog host anytime after adding it to the router configuration by entering the following command line:**

      $: set wfSyslogHostEntry.wfSyslogHostDisable.*<wfSyslogHostDest>* **2;commit**

      Disabling a host

      - Transitions the operational state of that Syslog host entry and its corresponding filters to INACTIVE
      - Stops Syslog from forwarding event messages to the host

   b. **Re-enable message forwarding to a specific Syslog host by entering the following command line:**

      $: set wfSyslogHostEntry.wfSyslogHostDisable.*<wfSyslogHostDest>* **1;commit**

      Re-enabling a host

      - Transitions the operational state of that Syslog host entry and its corresponding filters to ACTIVE
      - Allows Syslog to resume forwarding event messages to the host

2. **Disable or re-enable an entity filter for a specific Syslog host, as follows:**

   a. **Disable an entity filter anytime after adding it to the router configuration by entering the following command line:**

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrDisable. *<wfSyslogEntFltrHostIndex>.<wfSyslogEntFltrNum>.<wfSyslogEntFltrIndex>* **2;commit**

      Disabling a filter

      - Transitions the operational state of that filter (wfSyslogEntrFltrOperState) to INACTIVE
      - Stops Syslog from forwarding event messages through that filter

b. **Re-enable an entity filter by entering the following command line:**

$: set wfSyslogEntFltrEntry.wfSyslogEntFltrDisable. *<wfSyslogEntFltrHostIndex>.<wfSyslogEntFltrNum>.<wfSyslogEntFltrIndex>* **1;commit**

Re-enabling a filter

- Transitions the operational state of that filter (wfSyslogHostOperState) to ACTIVE
- Allows Syslog to resume forwarding event messages through that filter

Deleting Remote Hosts or Entity Filters from the Syslog Configuration

You can delete a remote host from the Syslog host table, or delete a filter from the Syslog filter table, as follows:

1. **If you want to delete a remote host entry from the Syslog host table, enter the following command line:**

   $: set wfSyslogHostEntry.wfSyslogHostDelete. *<wfSyslogHostDest>* **2;commit**

2. **If you want to delete a filter from the Syslog Entity Filter table, enter the following command line:**

   $: set wfSyslogEntFltrEntry.wfSyslogEntFltrDelete. *<wfSyslogEntFltrHostIndex>.<wfSyslogEntFltrNum>.<wfSyslogEntFltrIndex>* **2;commit**

3. **Save the changes to your configuration. (Refer to Task 8, earlier in this appendix.)**

Deleting Syslog from the Router

If you want to delete Syslog from the router, change the setting for wfSyslogDelete, a global parameter/attribute, as follows:

$:set wfSyslog.wfSyslogDelete.0 2;commit

Example Syslog Configuration

The following is an example of a Syslog configuration procedure when

- Your management workstation has an IP address of 192.32.6.14.
- You want to receive at your management workstation messages for all software entities running on a particular Bay Networks router. (This is a wildcard configuration scenario.)
- You want to create and enable Syslog on a model BLN router.
- You want to capture all fault, warning, and debug level messages from the router.
- You want to capture only messages logged on Slots 2 to 4 of the router.

Proceed as follows:

1. **Define a slot mask for Syslog on the router:**

   $: set wfProtocols.wfSYSLLoad.0 0x7FFE0000;commit

   The hexadecimal number 7FFE0000 converts to the binary number 0111 1111 1111 1110 0000 0000 0000 0000. The most significant bit position of the binary number represents Slot 1. The bit positions in descending order of significance represent Slots 2, 3, 4, etc.

2. **Create the Syslog base record on the router:**

   $: set wfSyslog.1.0 1;commit

3. **Create a host record for 192.32.6.14:**

   $: set wfSyslogHostTable.wfSyslogHostEntry.1.192.32.6.14 1;commit

Note: When you create a host record, the log facility defaults to a value of 184 (Local7).

4. **Create a wildcard filter to forward events of type fault, warning, and debug, and on Slots 2,3,4,5:**

   a. **Create the filter as follows:**

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrDelete. *<Host_IP_Address>***.255.1 1;commit**

      <Host_IP_Address> is the address of the remote host associated with this filter.

      255 is the wildcard entity number.

      1 represents the index number of the filter.

      commit commits router system resources to the filter you are creating.

   b. **Define the wildcard setting for filtering by event numbers.**

      The setting causes Syslog to ignore event numbers as a filtering criteria, and to use instead message severity levels as a filtering criteria.

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtLowBnd. 192.32.6.14.255.1 0

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtUppBnd. 192.32.6.14.255.1 255

   c. **Define a set of message severity levels (a "severity mask") that causes Syslog to select and forward only messages that have a severity level of fault, warning, or debug.**

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrSevMask. 192.32.6.14.255.1 "fwd"

      The next two commands define the range of Slots 2 to 4 (inclusive) as an additional filtering criterion. The commands cause Syslog to select only messages logged on Slots 2 to 5.

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowBnd. 192.32.6.14.255.1 2

      $: set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowUpp. 192.32.6.14.255.1 4

      $: commit

Note: If you add another filter for a specific entity, that filter takes precedence over the wildcard filter for the host you specified. At such time, the wildcard filter transitions to the INACTIVE state, the new filter transitions to the ACTIVE state, and the remote host receives messages only through the entity-specific filter.

Syslog Parameter Descriptions

Syslog objects and key parameters (attributes) that you can **set** on the router or **get** from the router by means of Technician Interface commands exist in the router MIB in the following hierarchy:

wfSyslog (group or global parameters pertaining to Syslog operation):

- wfSyslogDelete
- wfSyslogDisable
- wfSyslogOperState
- wfSyslogMaxHosts
- wfSyslogPollTimer

wfSyslogHostTable (table or list of remote host destinations for Syslog):

- **wfSyslogHostEntry** (individual remote host entry in the host table):
  - wfSyslogHostDelete
  - wfSyslogHostDisable
  - wfSyslogHostDest
  - wfSyslogHostUDPPort
  - wfSyslogHostLogFacility
  - wfSyslogTimeSeqEnable
  - wfSyslogHostOperState

wfSyslogEntityFilterTable (table of entity filters for one host):

wfSyslogEntFltrEntry (individual entity filter entry in the entity filter table):

wfSyslogEntFltrDelete

wfSyslogEntFltrDisable

wfSyslogEntFltrHostIndex

wfSyslogEntFltrNum

wfSyslogEntFltrIndex

wfSyslogEntFltrOperState

wfSyslogEntFltrLogEvtLowBnd

wfSyslogEntFltrLogEvtUppBnd

wfSyslogEntFltrSevMask

wfSyslogEntFltrSlotLowBnd

wfSyslogEntFltrSlotUppBnd

wfSyslogEntFltrFaultMap

wfSyslogEntFltrWarningMap

wfSyslogEntFltrInfoMap

wfSyslogEntFltrTraceMap

wfSyslogEntFltrDebugMap

For each attribute or parameter, this appendix provides information about default settings, valid options, function, instructions for setting, and the Management Information Base (MIB) object ID.

Global/Group Parameters

This section describes the Syslog group/global parameters.

Parameter:	**Syslog Delete**
Attribute Name:	wfSyslogDelete
Attribute Number:	1
Default:	1 (Create)
Options:	1 (Create) | 2 (Delete)
Function:	Creates or deletes the Syslog service on the router.
Instructions:	Set to 1 (Create) to create a MIB record with system defaults for the Syslog service on the router. Set to 2 (Delete) to delete the Syslog service from the router configuration.
Command:	**set wfSyslog.wfSyslogDelete.0** *<1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.1

Parameter:	**Enable**
Attribute Name:	wfSyslogDisable
Attribute Number:	2
Default:	(1) Enable
Options:	(1) Enable | (2) Disable
Function:	Enables or disables Syslog services on the router.
Instructions:	Enable Syslog services by also defining at least one remote host entry in the Syslog table (list) of hosts, and at least one entity filter for the remote host you define. Set to 2 (Disable) if you want to disable Syslog services on the router.
Command:	**set wfSyslog.wfSyslogDisable.0** *<1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.2

Parameter:	**Syslog Operational State**
Attribute Name:	wfSyslogOperState
Attribute Number:	3
Default:	1 (active)
Options:	1 (active) | (2) inactive
Function:	Indicates the operational state of the Syslog service on the router. If the state is active, syslog has been enabled, and is filtering and forwarding messages to designated hosts. If the state is inactive, Syslog is not filtering or forwarding messages for any of the following reasons: – Syslog has been disabled (wfSyslogDisable = 2). – No entries exist in the Syslog host table. – No entries in the Syslog host table have been enabled. – No entries enabled in the Syslog host table have any filters that have been enabled.
Instructions:	Examine the value of this attribute to determine the operational state of Syslog services on the router.
Command:	**get wfSyslog.wfSyslogOperState**
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.3

Parameter:	**Maximum Hosts**
Attribute Name:	wfSyslogMaxHosts
Attribute Number:	4
Default:	5
Range:	1 to 10
Function:	Specifies the maximum number of remote hosts considered “active” and able to receive messages from the Syslog service on the router. The number includes Syslog hosts configured to receive time-sequenced messages, as well as hosts configured to receive messages nonsequentially.
Instructions:	Enter the maximum number of active hosts allowed to receive messages from Syslog on the router. The actual number of entries in the host table can exceed the value of wfSyslogMaxHosts, but Syslog will forward messages only to the first “*n*” active hosts, where *n* equals the current setting of wfSyslogMaxHosts. Increasing the value of wfSyslogMaxHosts increases the overhead processing requirements for Syslog on the router.
Command:	**set wfSyslog.wfSyslogMaxHosts.0** *<1 - 10>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.4

Parameter:	**Log Poll Timer**
Attribute Name:	WfSyslogPollTimer
Attribute Number:	5
Default:	5 seconds
Range:	5 to 610000
Function:	Determines the amount of time Syslog waits before initiating another cycle to poll all slots for event messages logged since the previous polling cycle.
Instructions:	Enter the number of seconds that you want Syslog to wait between polling cycles.
Command:	**set wfSyslog.wfSyslogPollTimer.0** *<5 - 610000>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.1.5

Host Parameters

This section describes parameters you can configure for each host you add to the Syslog host table (list of remote UNIX hosts).

Parameter:	**Host Delete**
Attribute Name:	wfSyslogHostDelete
Attribute Number:	1
Default:	1 (Create)
Options:	1 (Create) | 2 (Delete)
Function:	Adds or deletes a remote host entry in the Syslog host table. Parameters associated with this entry collectively define a remote host that will receive Syslog (event) messages from the router.
Instructions:	Set to 1 to add a host to the Syslog host table. Set to 2 to delete a host from the Syslog host table.
Command:	**set wfSyslogHostEntry.wfSyslogHostDelete.***<host_IP_address> <1 | 2>*

Parameter:	**Messaging Enable**
Attribute Name:	wfSyslogHostDisable
Attribute Number:	2
Default:	1 (Enable)
Options:	1 (Enable) | 2 (Disable)
Function:	Enables or disables message forwarding from Syslog to the remote host associated with this host entry.
Instructions:	Set to 1 to enable message forwarding from Syslog to the remote host associated with this host entry. Set to 2 to disable message forwarding from Syslog to the remote host associated with this host entry. You can also stop forwarding router events to the host by deleting the host. (Refer to the Host Delete parameter, wfSyslogHostDelete.) If you delete a remote host and later decide you want to forward router events to that host, you must add the remote host again to the Syslog host table.
Command:	**set wfSyslogHostEntry.wfSyslogHostDisable.***<host_IP_address> <1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.2

Parameter:	**Host UDP Port**
Attribute Name:	wfSyslogHostUDPPort
Attribute Number:	4
Default:	514
Range:	514 to 530
Function:	Identifies the UDP port of the remote host associated with this host entry.
Instructions:	Set (designate) the UDP port at which the remote host associated with this host entry will receive Syslog (event) messages from the router.
Command:	**set wfSyslogHostEntry.wfSyslogHostUDPPort.***<host_IP_address> <514 - 530>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.4

Parameter:	**Host Log Facility**
Attribute Name:	wfSyslogHostLogFacility
Attribute Number:	5
Default:	184 (LOCAL7)
Options:	128 (LOCAL0 136 (LOCAL1) 144 (LOCAL2) 152 (LOCAL3) 160 (LOCAL4) 168 (LOCAL5) 176 (LOCAL6) 184 (LOCAL7)
Function:	Specifies the UNIX system facility that receives and dispatches Syslog (event) messages from the router.
Instructions:	Set (designate) the facility that you want the remote host to use for receiving and dispatching Syslog (event) messages from the router. Designate the same facility in the *syslog.conf* file on the remote host.
Command:	**set wfSyslogHostEntry.wfSyslogHostLogFacility.** *<host_IP_address> <128 | 136 | 144 | 152 | 160 | 168 | 176 | 184>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.5

Parameter:	**Host Time Seq Enable**
Attribute Name:	wfSyslogLogTimeSeqEnable
Attribute Number:	6
Default:	2 (Disable)
Options:	1 (Enable) | 2 (Disable)
Function:	Enables or disables time sequencing and forwarding of Syslog (event) messages to the remote host associated with this host entry.
Instructions:	Enable this feature only if it is essential for the remote host to receive Syslog (event) messages in the order in which they were logged on the router. When you enable this feature, Syslog on each slot – Polls the local events log – Retrieves messages from the local log – Filters the messages – Time-sequences messages that pass through the filters – Forwards sequenced messages to IP on the router, which in turn forwards the messages to the remote host associated with this entry When you disable this feature, Syslog on each slot – Polls the local events log – Retrieves messages from the local log – Filters the messages – Forwards sequenced messages to IP on the router, which in turn forwards the messages to the remote host associated with this entry
Command:	**set wfSyslogHostEntry.wfSyslogLogTImeSeqEnable.** *<host_IP_address> <1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.6

Parameter:	**Host Operational State**
Attribute Name:	wfSyslogHostOperState
Attribute Number:	7
Default:	2 (inactive host)
Options:	1 (active) | 2 (inactive)
Function:	Indicates the operational state of this Syslog host entry on the router. If the state is active, Syslog is filtering and forwarding messages to the host at the IP address for this entry (<*wfSyslogHostDest*>). If the state is inactive, Syslog is not filtering or forwarding messages for any of the following reasons: – Syslog has been disabled (wfSyslogDisable = 2). – This entry in the Syslog host table has been disabled. – This entry has no configured filters. – No filter entries for this host are active. – Too many Syslog host entries are already active. (The number of configured hosts is greater than the value of wfSyslogMaxHosts.)
Instructions:	Examine the value of wfSyslogHostOperState to determine whether or not Syslog is forwarding any messages to the host associated with this wfSyslogHostEntry.<*instance_id*>.
Command:	**get wfSyslogHostEntry.wfSyslogHostOperState.**<*wfSyslogHostDest*>
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.2.1.7

Entity Filter Parameters

This section describes the parameters you can configure for each filter (entry) you add to the Syslog entity filter table.

Parameter:	**Entity Filter Delete**
Attribute Name:	wfSyslogEntFltrDelete
Attribute Number:	1
Default:	1 (Create)
Options:	1 (Create) | 2 (Delete)
Function:	Creates or deletes an entity filter for the remote host at the location defined by wfSyslogEntFltrHostIndex for this filter table entry.
Instructions:	Set to 1 to create an entity filter for the remote host at the IP address defined by wfSyslogEntFltrHostIndex for this filter table entry. Set to 2 to delete this entity filter.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrDelete.** *<host_IP_address>.<entity_code>.<filter_index> <1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.1

Parameter:	**Entity Filter Enable**
Attribute Name:	wfSyslogEntFltrDisable
Attribute Number:	2
Default:	(1) Enable
Options:	(1) Enable | (2) Disable
Function:	Enables or disables the entity filter associated with this filter table entry.
Instructions:	Set to 1 to enable the entity filter associated with this filter table entry. Set to 2 to disable the entity filter associated with this filter table entry.
Command:	**set wfSyslogHostEntry.wfSyslogEntFltrDisable.** *<host_IP_address>.<entity_code>.<filter_index> <1 | 2>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.2

Parameter:	**Filter Operational State**
Attribute Name:	wfSyslogEntFltrOperState
Attribute Number:	6
Default:	2 (inactive filter)
Options:	1 (active filter) | 2 (inactive filter)
Function:	Indicates the actual status of the filter. When the status is ACTIVE, Syslog is filtering against the criteria specified for this filter. When the state is INACTIVE, Syslog is not using this filter to select and forward messages to a remote host for one or more of the following reasons: – Filter's host is not ACTIVE. – Filter does not have a configured event number or range. – Filter does not have a configured severity mask. – Filter slot number(s) do not correspond to actual slot numbers on this model of router.
Instructions:	Retrieve the value of this attribute when you want to check the status of a filter for a specific entity.
Command:	**get wfSyslogEntFltrEntry.wfSyslogEntFltrOperState**
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.6

Parameter:	**Log Evt Lower Bound**
Attribute Name:	wfSyslogEntFltrLogEvtLowBnd
Attribute Number:	7
Default:	0
Range:	0 to 255
Function:	Along with the Log Evt Upper Bound, this parameter/attribute specifies an event number (code) or range of event numbers. The number(s) correspond to event messages you want to forward to the remote host associated with this filter. For a complete list of event codes for each entity, refer to *Event Messages for Routers and BNX Platforms* for this version of the router software.
Instructions:	To specify a range of event numbers that identify messages you want to forward to a remote host, set the value of this parameter/attribute to the low number of the range. Set the value of the wfSyslogEntFltrLogEvtUppBnd (Log Event Upper Bound) parameter to the high number of the range. Any range you specify includes the values for the lower and upper bound parameters/attributes. For example, if you specify a lower bound of 2 and an upper bound of 7, Syslog forwards all messages with event codes of 2 through 7 (inclusive), logged by the entity defined under wfSyslogEntFltrNum (Filter Entity Name). Syslog ignores all other event messages. To filter (select only) a specific event, set the value of wfSyslogEntFltrLogEvtLowBnd to the code number for that event. Set the value of wfSyslogEntFltrLogEvtUppBnd (Log Evt Upper Bound) to the same code number. For example, to forward only log messages that have an event code of 10, enter 10 as the value of wfSyslogEntFltrLogEvtLowBnd and as the value of the wfSyslogEntFltrLogEvtUppBnd (Log Evt Upper Bound). If you do not want to filter by event code, accept the lower and upper bound default values of 0 to 255. In this case, Syslog checks for filtering criteria based on a message severity mask (wfSyslogEntFltrSevMask). If you specify lower and upper boundary values of 255 (the wildcard entity number), Syslog ignores this attribute as filtering criterion.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtLowBnd.** *<host_IP_address>.<entity_code>.<filter_index> <0 - 255>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.7

Parameter:	**Log Evt Upper Bound**
Attribute Name:	wfSyslogEntFltrLogEvtUppBnd
Attribute Number:	8
Default:	255
Range:	0 to 255
Function:	Along with the Log Evt Lower Bound, this parameter/attribute specifies an event number (code) or range of event numbers. The number(s) correspond to event messages you want to forward to the remote host associated with this filter. For a complete list of event codes for each entity, refer to *Event Messages for Routers and BNX Platforms* for this version of the router software.
Instructions:	To specify a range of event numbers that identify messages you want to forward to a remote host, set the value of this parameter/attribute to the high number of the range. Set the value of the wfSyslogEntFltrLogEvtLowBnd (Log Event Upper Bound) parameter to the low number of the range. Any range you specify includes the values for the lower and upper bound parameters/attributes. For example, if you specify a lower bound of 2 and an upper bound of 7, Syslog forwards all messages with event codes of 2 through 7 (inclusive), logged by the entity defined under wfSyslogEntFltrNum (Filter Entity Name). Syslog ignores all other event messages. To filter (select only) a specific event, set the value of wfSyslogEntFltrLogEvtUppBnd to the code number for that event. Set the value of wfSyslogEntFltrLogEvtLowBnd (Log Event Lower Bound) to the same code number. For example, to forward only log messages that have an event code of 10, enter 10 as the value of wfSyslogEntFltrLogEvtUppBnd and as the value of the wfSyslogEntFltrLogEvtLowBnd (Log Event Lower Bound). If you do not want to filter by event code, accept the upper and lower boundary default values of 0 and 255. In this case, Syslog checks for filtering criteria based on a message severity mask (wfSyslogEntFltrSevMask). If you specify lower and upper boundary values of 255 (the wildcard entity number), Syslog ignores this attribute as filtering criterion.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrLogEvtUppBnd.** *<host_IP_address>.<entity_code>.<filter_index> <0 - 255>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.8

Parameter:	**Severity Mask**
Attribute Name:	wfSyslogEntFltrSevMask
Attribute Number:	9
Default:	None
Options:	w (warning) i (information) t (trace) f (fault) d (debug) Use individually (such as **f** or **d**) or combined (such as **fwitd**).
Function:	Identifies the severity levels (warning, informational, trace, fault, debug) of events you want to forward. Syslog uses this severity mask as filtering criteria only if you specify the wildcard event number range (0 - 255) as the values for wfSyslogEntFltrLogEvtLowBnd and wfSyslogEntFltrLogEvtUppBnd. Syslog looks only for events that have the severity levels you specify.
Instructions:	If you specify a range of event numbers (using the Log Evt Lower Bound and Log Evt Upper Bound parameters), Syslog ignores the Severity Mask parameter. If you do not specify a range of event numbers, Syslog applies the value of the Severity Mask attribute to the current filter. Enter the severity level identifiers of event messages you want to forward to the remote host associated with this filter. Use the first letter of each event severity level you want to include: f - fault w - warning i - information t - trace d- debug Enter lowercase letters only. Do not separate the letters with commas or spaces.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrSevMask.** *<host_IP_address>***.***<entity_code>***.***<filter_index>* *<witfd>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.9

Parameter:	**Slot Lower Bound**
Attribute Name:	wfSyslogEntFltrSlotLowBnd
Attribute Number:	10
Default:	0
Range:	0 to 14
Function:	Along with the Slot Upper Bound, this parameter/attribute specifies a slot number or range of slot numbers. Syslog forwards to the remote host associated with this filter messages logged only on the slot(s) you specified. (Consider the location of each router in an ASN chassis as a numbered slot.)
Instructions:	To specify a range of slots, set the value of this parameter/attribute to the low number of the range. Also set the value of wfSyslogEntFltrSlotUppBnd (Slot Upper Bound) to the higher number of the range. Any range you specify includes the values for the lower and upper bound parameters/attributes. For example, if you specify a lower bound of 1 and an upper bound of 4, Syslog forwards all event messages logged on Slots 1 through 4 (inclusive). Syslog ignores all other event messages. To filter events for a specific slot, set the value of wfSyslogEntFltrSlotLowBnd to the desired slot number. Set the value of wfSyslogEntFltrSlotUppBnd to the same number. For example, to forward only event messages logged on Slot 2, enter 2 as the value of wfSyslogEntFltrSlotLowBnd and as the value of wfSyslogEntFltrSlotUppBnd. If you do not want to filter messages by slot number(s), accept the lower and upper bound default values of 0.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotLowBnd.** *<host_IP_address>.<entity_code>.<filter_index> <0 - 14>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.10

Parameter:	**Slot Upper Bound**
Attribute Name:	wfSyslogEntFltrSlotUppBnd
Attribute Number:	11
Default:	0
Range:	0 to 14
Function:	Along with the Slot Lower Bound, this parameter/attribute specifies a slot number or range of slot numbers. Syslog forwards to the remote host associated with this filter messages logged only on the slot(s) you specified. (Consider the location of each router in an ASN chassis as a numbered slot.)
Instructions:	To specify a range of slots, set the value of this parameter/attribute to the high number in the range. Also set the value of wfSyslogEntFltrSlotLowBnd (Slot Lower Bound) to the low number of the range. Any range you specify includes the values for the lower and upper bound parameters/attributes. For example, if you specify a lower bound of 1 and an upper bound of 4, Syslog forwards all event messages logged on Slots 1 through 4 (inclusive). Syslog ignores all other event messages. To filter events for a specific slot, set the value of wfSyslogEntFltrSlotLowBnd to the desired slot number. Set the value of wfSyslogEntFltrSlotUppBnd to the same number. For example, to forward only event messages logged on Slot 2, set the value of wfSyslogEntFltrSlotLowBnd and wfSyslogEntFltrSlotUppBnd to 2. If you do not want to filter messages by slot number(s), accept the lower and upper bound default values of 0.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrSlotUppBnd.** *<host_IP_address>.<entity_code>.<filter_index> <0 - 14>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.3.1.11

Parameter:	**Fault Map**
Attribute Name:	wfSyslogEntFltrFaultMap
Attribute Number:	12
Default:	3 (CRIT)
Options:	1 (EMERG) | 2 (ALERT) | 3 (CRIT) | 4 (ERR) | 5 (WARNING) | 6 (NOTICE) | 7 (INFO) | 8 (DEBUG)
Function:	Maps router event messages with a severity level of fault to a UNIX system error level that Syslogd recognizes. Table C-1 describes each of these error levels.
Instructions:	We recommend accepting the default UNIX system error level for this severity level. To map this severity level to a different UNIX system error level, set wfSyslogEntFltrFaultMap to the error level you want.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrFaultMap.***<host_IP_address>***.***<entity_code>***.***<filter_index>* *<1 | 2 | 3 | 4 | 5 | 6 | 7 | 8>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.4.1.12

Table C-1. Syslogd Error Levels

Error Level	Description
EMERG	A panic condition that *syslogd* normally broadcasts to all users.
ALERT	A condition that you should correct immediately, such as a corrupted system database.
CRIT	Critical conditions, such as hard device errors.
ERR	Errors.
WARNING	Warning messages.
NOTICE	Conditions that are not errors but may require special handling.
INFO	Informational messages.
DEBUG	Messages that contain information you can use when debugging or troubleshooting your network.

Parameter:	**Warning Map**
Attribute Name:	wfSyslogEntFltrWarningMap
Attribute Number:	13
Default:	5 (WARNING)
Options:	1 (EMERG) | 2 (ALERT) | 3 (CRIT) | 4 (ERR) | 5 (WARNING) | 6 (NOTICE) | 7 (INFO) | 8 (DEBUG)
Function:	Maps router event messages with a severity level of warning to a UNIX system error level that Syslogd recognizes. Table C-1 describes each of these error levels.
Instructions:	We recommend accepting the default UNIX system error level for this severity level. To map this severity level to a different UNIX error level, set wfSyslogEntFltrWarningMap to the error level you want.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap.** *<host_IP_address>.* *<entity_code>.<filter_index>* *<1|2|3|4|5|6|7|8>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.4.1.13

Parameter:	**Info Map**
Attribute Name:	wfSyslogEntFltrInfoMap
Attribute Number:	14
Default:	7 (INFO)
Options:	1 (EMERG) | 2 (ALERT) | 3 (CRIT) | 4 (ERR) | 5 (WARNING) | 6 (NOTICE) | 7 (INFO) | 8 (DEBUG)
Function:	Maps router event messages with a severity level of info to a UNIX system error level that Syslogd recognizes. Table C-1 describes each of these error levels.
Instructions:	We recommend accepting the default UNIX system error level for this severity level. To map this severity level to a different UNIX error level, set wfSyslogEntFltrInfoMap to the error level you want.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrInfoMap.** *<host_IP_address>.* *<entity_code>.<filter_index>* *<1|2|3|4|5|6|7|8>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.4.1.14

Parameter:	**Trace Map**
Attribute Name:	wfSyslogEntFltrTraceMap
Attribute Number:	15
Default:	8 (DEBUG)
Options:	1 (EMERG) | 2 (ALERT) | 3 (CRIT) | 4 (ERR) | 5 (WARNING) | 6 (NOTICE) | 7 (INFO) | 8 (DEBUG)
Function:	Maps router event messages with a severity level of trace to a UNIX system error level that Syslogd recognizes. Table C-1 describes each of these error levels.
Instructions:	We recommend accepting the default UNIX error level for this severity level. To map this severity level to a different UNIX error level, set wfSyslogEntFltrTraceMap to the error level you want.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrTraceMap.***<host_IP_address>***.***<entity_code>***.***<filter_index>* *<1|2|3|4|5|6|7|8>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.4.1.15

Parameter:	**Debug Map**
Attribute Name:	wfSyslogEntFltrDebugMap
Attribute Number:	16
Default:	8 (DEBUG)
Options:	1 (EMERG) | 2 (ALERT) | 3 (CRIT) | 4 (ERR) | 5 (WARNING) | 6 (NOTICE) | 7 (INFO) | 8 (DEBUG)
Function:	Maps router event messages with a severity level of debug to an error level that UNIX Syslogd recognizes. Table C-1 describes each of these error levels.
Instructions:	We recommend accepting the default UNIX system error level for this severity level. To map this severity level to a different UNIX system error level, set wfSyslogEntFltrDebugMap to the error level you want.
Command:	**set wfSyslogEntFltrEntry.wfSyslogEntFltrDebugMap.***<host_IP_address>***.***<entity_code>***.***<filter_index>* *<1|2|3|4|5|6|7|8>*
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.15.4.1.16

For More Information

Refer to the instructions provided in the UNIX man(ual) pages on your workstation for more information on *syslog*, *syslogd*, and *syslog.conf*.

Index

Symbols

! command, 3-3

* wildcard, 5-2

? wildcard, 5-2

A

aborting a command, 3-3

access
- levels
  - manager, 8-78 to 8-81
  - user, 8-78 to 8-81
- password protection, 1-3
- via SecureID, 1-3

ACE
- backplane, 8-46
- processor module, 4-4

ace.out image, 4-4

ace.out image file, 4-9

afn.exe image, 4-4

afn.exe image file, 4-9

afnboot.exe PROM image file, 4-9

alias command, 9-2

aliases
- creating, 9-2
- debugging, 9-7
- debugging network problems with predefined, 9-10
- definition of, 9-1
- deleting from memory, 9-7
- displaying, 9-2
- file, 4-10
- in debug.al file, 9-10 to 9-18
- inserting character strings in, 9-5
- inserting parameters in, 9-3
- loading from a file, 9-9
- managing, 9-1 to 9-18
- saving to a file, 9-8

an.exe image, 4-9

an.exe image file, 4-4

AN/ASN
- configuring boot and config file source, 8-2 to 8-8

anboot.exe PROM image file, 4-9

andiag.exe PROM image file, 4-9

APING, 3-24

AppleTalk ping command, 3-21 to 3-23

applications, viewing addresses and sizes of, 8-44

APPN ping command, 3-24 to 3-26

asn.exe image, 4-9

asn.exe image file, 4-4

asnboot.exe, 4-9

asnboot.exe PROM image file, 4-9

asndiag.exe PROM image file, 4-9

atmarp command, 3-27

attr command, 5-19 to 5-20

attributes. *See* parameters

audience for this guide, xx

autosave, log, 6-10

Autoscript parameters
Force User Logout, 2-17
Login Script Search Path, 2-15
Manager's Login Script, 2-15
User's Login Script, 2-16
autoscripts
at manager login, 2-20
at user login, 2-20
automgr.bat, 2-19 to 2-20
autouser.bat, 2-19 to 2-20
customizing, 2-21
samples, 2-20

B

backplane
command, 8-46
setting the, 8-46
baud rate, setting, 2-8
Bay Networks
CompuServe forum, xxx
Customer Service FTP, xxix
home page on World Wide Web, xxix
InfoFACTS service, xxxi
publications, ordering, xxiii
support programs, xxviii
Support Source CD, xxx
Technical Response Center, xxvii, xxxi
technical support, xxvii
bconfig command, 8-3 to 8-4
bn.exe image, 4-4, 4-9
boot
after graceful shutdown, 8-13
command, 8-9 to 8-12
delayed, 8-14
router, 8-9 to 8-13
BOOTP server, 8-7, 8-8
broadcast addresses, 3-8

C

cd command, 4-10, 5-7
clearlog command, 6-14
CLNP echo request, 3-15
clocking, 8-6
commands
aborting, 3-3
access levels, 8-78 to 8-81
alias management
alias, 9-2
echo, 9-5
save aliases, 9-8
source aliases, 9-9
unalias, 9-7
verbose, 9-7
atmarp, 3-27
bconfig, 8-3 to 8-4
DOS
attr, 5-19 to 5-20
cd, 5-7
copy, 5-14
delete, 5-21
dir, 5-8
label, 5-11
mkdir, 5-12
mount, 5-4
rename, 5-13
rmdir, 5-12
tftp, 5-16
type, 5-20
unmount, 5-6
history, 3-4
ifconfig, 8-5 to 8-8
issuing, 3-1

MIB
commit, 2-4, 7-8
get, 7-4
list, 7-2
save config, 7-9
set, 7-6
wfsnmpkey, 8-54
wfsnmpmode, 8-53
wfsnmpseed, 8-54
NVFS
cd, 4-10
compact, 4-19
copy, 4-11
delete, 4-18
dinfo, 4-6
dir, 4-7
format, 4-20
partition, 4-21
tftp, 4-14
type, 4-17
out-of-band file transfer
tip, B-1, B-10
xmodem, B-1, B-4
Technician Interface operating
backplane, 8-46
boot, 8-9
clearlog, 6-14
date, 8-46
diags, 8-29
exec, 3-7
help, 3-2
history, 3-4
ifconfig, 8-5
loadmap, 8-44
log, 6-6, 6-13
logout, 1-12
more, 3-2
password, 8-49
ping AppleTalk, 3-21 to 3-23
ping APPN, 3-24 to 3-26
ping IP, 3-8 to 3-11
ping IPX, 3-12 to 3-14
ping OSI, 3-15 to 3-17
ping VINES, 3-18 to 3-20
prom, 8-33, 8-38
readexe, 8-33 to 8-35
record, 8-60
repeat (!), 3-3
reset, 8-24
restart, 8-22
save log, 6-8
stamp, 8-32
stop, 8-33
system, 1-13
timeout condition, 2-14
commit command, 2-4, 7-8
compact command, 4-19
compression
file, 8-37
hardware, 8-55
CompuServe, Bay Networks forum on, xxx
config file, 4-9, 8-10
configuring
AN/ASN boot and config file source, 8-8
for Telnet access, 1-12
log autosave, 6-10
the console port, 1-12
configuring Syslog on a router, C-15
connection
dial-in to router, 1-1
telnet to router, 1-1
console port parameters, 2-4
Autosave Volume, 2-18
Baud Rate, 2-8
Command Timeout, 2-14
Data Bits, 2-9
Delete, 2-5
Disable, 2-5
Force User Logout, 2-17
History Depth, 2-17
Lines Per Screen, 2-11
Login Retries, 2-14
Login Script Search Path, 2-15
Login Timeout, 2-13
Manager’s Login Script, 2-15
Maximum Autosaved Files, 2-18

Modem Enable, 2-10
More, 2-11
Password Timeout, 2-13
Port Name, 2-7
Port Number, 2-6
Port Parity, 2-9
Port Type, 2-8
Slot Number, 2-7
State, 2-6
Stop Bits, 2-10
User's Login Script, 2-16
Control Point name, 3-24
copy command, 4-11, 5-14
Customer Service FTP, xxix
customer support. *See* getting help

D

data bits, setting, 2-9
date command, 8-46
debug aliases, 9-10 to 9-18
debug.al file, 4-10
default filenames, 4-9
default settings, IP interface, 8-7
delayed boot, 8-14
delete command, 4-18, 5-21
deleting a console port instance, 2-5
diagnostics, running, 8-29
diags command, 8-9 to 8-10, 8-29
dial connection to router, 1-1
dinfo command, 4-6
dir command, 4-7, 5-8
directed boot, 8-11
Directed Netboot
configuring with bconfig command, 8-4
directories
changing, 5-7
creating, 5-12
displaying, 5-8
removing, 5-12
renaming, 5-13
disable command, 1-13
disabling
a console port, 2-5
Syslog hosts or filters, C-24
the Syslog entity, C-23
display filters, events log, 6-6
DLCMI settings, 8-6
DOS
file attributes, 5-19
file system
labeling a diskette, 5-11
managing using the Technician Interface, 5-2 to 5-22
naming files and directories, 5-3

E

echo command, 9-5
enable command, 1-13
enabling internal clock mode, 8-62
encryption key, setting, 8-54
End of File marker, 5-6
entity filters
for Syslog remote hosts, C-5
events (via Events Manager)
clearing, 6-14
displaying filters, 6-5
displaying log for, 6-2, 6-13
filtering log input, 6-3
filtering log output, 6-6
managing, 6-2 to 6-14
saving log for, 6-8

events (via Syslog). *See* Syslog
exec command, 3-7
executable files, 4-4, 8-34

F

FIFO memory buffer, 6-2
File Allocation Table, 5-6
file attributes, 5-19
File System Check Report, 5-5 to 5-6
files
  ace.out, 4-9
  afn.exe, 4-9
  afnboot.exe, 4-9
  an.exe, 4-9
  anboot.exe, 4-9
  andiag.exe, 4-9
  asn.exe, 4-9
  asndiag.exe, 4-9
  bn.exe, 4-9
  changing attributes of, 5-19
  compacting space, 4-19
  config, 4-9
  copying, 4-11, 5-14
    from DOS to NVFS, 5-15
    from NVFS to DOS, 4-11
  debug.al, 4-10
  default names of, 4-9
  deleting, 4-18, 5-21
  displaying the contents of, 4-17, 5-20
  freboot.exe, 4-10
  install.bat, 4-10
  names, 4-5
  renaming, 5-13
  syslog.conf, C-47
  ti.cfg, 4-10
  transferring, 4-13, 5-15
    to full memory card, 4-20
  validating an executable, 8-35
filters
  events log input, 6-3
  events log input filters, displaying, 6-5
  events log output, 6-6
  Syslog, C-4
Flash System Controller, 4-2
Force User Logout parameter, 2-17
format command, 4-20
Frame Relay
  settings, 8-6
FRE processor module, 4-2, 4-4
freboot.exe PROM image file, 4-10
frediag.exe PROM image file, 4-10

G

get command, 7-4
getting help
  from a Bay Networks Technical Response Center, xxxi
  from the Support Source CD, xxx
  through CompuServe, xxx
  through Customer Service FTP, xxix
  through InfoFACTS service, xxxi
  through World Wide Web, xxix
graceful shutdown (BNX), 8-13, 8-23, 8-28

H

hardware compression, 8-55
hardware configuration, for out-of-band file transfers, B-9
HDLC encapsulation, 8-6
help
  command, 3-2
  displaying online, 3-2
history
  command, 3-4
  list, changing the size of the, 3-4

I

ICMP echo request, 3-8
ifconfig command, 8-5 to 8-8
images, 4-4
  ace.out, 4-4, 4-9, 5-4
  afn.exe, 4-9
  afnboot.exe, 4-9
  anboot.exe, 4-9
  andiag.exe, 4-9
  asnboot.exe, 4-9
  asndiag.exe, 4-9
  bn.exe, 5-4
  freboot.exe, 4-10
  frediag.exe, 4-10
  list, 4-4, 4-9
in-band file transfers
  DOS, 5-16 to 5-18
  NVFS, 4-14 to 4-16
InfoFACTS service, xxxi
initializing the Technician Interface, 1-3
install.bat file, 4-10, 5-11
interface configuration, 8-5 to 8-8
internal clock mode, enabling, 8-62
IP
  address settings, 8-7, 8-8
  connector setting, 8-6, 8-7
  default setting, 8-6, 8-7
  ping command, 3-8 to 3-11
IPX ping command, 3-12 to 3-14

L

label command, 5-11
lines per screen, setting, 2-11
list command, 2-2, 7-2
loadmap command, 8-44
log
  automatically saving the, 6-10
  command, 6-6, 6-13
  input filters, 6-3
    displaying list of, 6-5
  ouput filters, 6-6
login
  levels, 1-3
  Manager's Script, 2-15
  procedure, 1-3
  retries, 2-14
  script search path, 2-15
  timeout, 2-13
  timeout guidelines, 1-11
  User's Script, 2-16
  with password, 1-4
  with Secure ID, 1-5
Login Script Search Path, 2-15
logout
  command, 1-12
  setting, 2-17
loopback, 3-8

M

Management Information Base. *See* MIB
manager session
  command access levels, 8-78 to 8-81
  starting from within user session, 1-13
  terminating, 1-12
Manager's Login Script parameter, 2-15
Manager's login script, setting, 2-15
memory
  buffer, 6-2
  displaying the status of volumes, 4-6
  formatting, 4-20
  partitioning, 4-21
  transferring files to a full card, 4-20
  using multiple cards, 4-3
menu command, 1-13

messages
mapping router events to Syslog format, C-8
time-sequencing Syslog, C-35
MIB, 1-13
accessing, 7-1 to 7-8
Bay Networks files, A-7
committing sets, 7-8
compliance with specifications, A-7
getting values, 7-4 to 7-6
implementation notes, A-8 to A-10
listing objects, 7-2 to 7-4
setting values, 7-6 to 7-8
structure of, A-2 to A-5
using, A-1 to A-10
MIB-II counter, 7-9
mkdir command, 5-12
modem, enabling a, 2-10
monitor command, 1-13
more command, 3-2
Motorola processor module, 4-4
mount command, 5-4

N

named boot, 8-11
NLSP ping response, 3-12
Non-Volatile File System. *See* NVFS
NSAP address, 3-15
NVFS, 4-5

O

online help, 3-2
operational state
of a Syslog filter, C-38
of a Syslog host, C-36
of the Syslog entity, C-31
OSI ping command, 3-15 to 3-17
out-of-band file transfers
from a UNIX workstation, B-10 to B-16
from a Windows workstation, B-17 to B-31
hardware configuration, B-9
overview of, B-1 to B-2
overwriting files, 5-14, 5-17

P

packet transfer, halting between slots, 8-33
parameters
Console
Baud Rate, 2-8
Command Timeout, 2-14
Data Bits, 2-9
Force User Logout, 2-17
Lines Per Screen, 2-11
Login Retries, 2-14
Login Script Search Path, 2-15
Login Timeout, 2-13
Manager's Login Script, 2-15
Modem Enable, 2-10
More Enable, 2-11
Password Timeout, 2-13
Port Delete, 2-5
Port Disable, 2-5
Port Name, 2-7
Port Number, 2-6
Port Parity, 2-9
Port Slot, 2-7
Port State, 2-6
Port Type, 2-8
Stop Bits, 2-10
User's Login Script, 2-16
Syslog
Debug Map, C-46
Entity Filter Delete, C-37
Entity Filter Enable, C-37
Fault Map, C-44
Filter Operational State, C-38
Host Delete, C-33
Host Log Facility, C-34
Host Operational State, C-36
Host Time Seq Enable, C-35

Host UDP Port, C-34
Info Map, C-45
Log Evt Lower Bound, C-39
Log Evt Upper Bound, C-40
Maximum Hosts, C-32
Messaging Enable, C-33
Operational State, C-31
Severity Mask, C-41
Slot Lower Bound, C-42
Slot Upper Bound, C-43
Syslog Delete, C-30
Syslog Enable, C-30
Syslog Log Poll, C-32
Trace Map, C-46
Warning Map, C-45

partition command, 4-21

password
access, 1-3
assigning a, 8-48
command, 8-49
for new systems, 1-4
setting timeout for, 2-13

path trace report, 3-8

pausing and scrolling the screen, 3-2

PCMCIA/Floppy switch, 8-12 to 8-13

ping command
AppleTalk, 3-21 to 3-23
APPN, 3-24 to 3-26
IP, 3-8 to 3-11
IPX, 3-12 to 3-14
IPX, NLSP response, 3-12
OSI, 3-15 to 3-17
VINES, 3-18 to 3-20

pinging a remote device, 3-7 to 3-26

platform key, 8-37

port
name, displaying the, 2-7
number, displaying the, 2-6
parity setting, 2-9
type, displaying the, 2-8

processor modules, 4-4

prom
command, 8-33, 8-38
verifying and upgrading software on, 8-38

protected access
via password, 1-3
via SecureID, 1-3

Q

QENET underflow errors, 8-62

R

readexe command, 8-33 to 8-38

record command, 8-60

recording console messages to a file, 8-60

rename command, 5-13

repeat command (!), 3-3

repeating a Technician Interface command, 3-3, 3-4

reset after graceful shutdown, 8-28

reset command, 8-9 to 8-10, 8-24

restart after graceful shutdown, 8-23

restart command, 8-22

rmdir command, 5-12

router software images, 4-4

S

save aliases command, 9-8

save command, 2-4

save config command, 7-9, 8-3

save log command, 6-8

saving the log automatically, 6-10

screen pauses, setting, 2-11

scripts, Technician Interface, 1-2, 1-13

scrolling the Technician Interface screen, 3-2

secure mode, managing, 8-52 to 8-55

SecurID
access, 1-3
login and PIN assignment, 1-6
security counter, resetting, 8-54
set command, 2-3, 7-6
show command, 1-13
Site Manager, 1-2
slot
number, displaying the, 2-7
resetting, 8-24
restarting, 8-22
Technician Interface running on, 1-3
software
displaying version, 8-32
upgrading, 8-33
verifying, 8-33
source aliases command, 9-9
Spanning Tree, 7-7
SRM-L board, 2-1 to 2-2
stamp command, 8-32
Standard Point-to-Point protocol, 8-6
state of a console port, displaying the, 2-6
stop bits, setting, 2-10
stop command, 8-33
Support Source CD, xxx
SYS I/O board, 2-1 to 2-2
Syslog
configuring the router for, C-15
deleting from router, C-25
deleting remote hosts or filters, C-25
disabling or re-enabling, C-23
disabling or re-enabling remote hosts or filters, C-24
entity filter parameters, C-37
example configuration, C-26
global parameters/attributes, C-30
IP header, C-9
mapping router events to Syslog format, C-8
message filtering diagram, C-5
parameter descriptions, C-28
parameters
Debug Map, C-46
Delete, C-30
Enable, C-30
Entity Filter Delete, C-37
Entity Filter Enable, C-37
Fault Map, C-44
Filter Operational State, C-38
Host Delete, C-33
Host Log Facility, C-34
Host Operational State, C-36
Host Time Seq Enable, C-35
Host UDP Port, C-34
Info Map, C-45
Log Evt Lower Bound, C-39
Log Evt Upper Bound, C-40
Log Poll, C-32
Maximum Hosts, C-32
Messaging Enable, C-33
Operational State, C-31
Severity Mask, C-41
Slot Lower Bound, C-42
Slot Upper Bound, C-43
Trace Map, C-46
Warning Map, C-45
remote host address, C-9
Remote Host Parameters, C-33
syslog.conf file (on UNIX workstation), C-13
system command, 1-13

T

Technician Interface
accessing via ASCII terminal, 1-2
accessing via Telnet connection, 1-2
establishing multiple sessions, 2-2
initializing, 1-3
logging out, 1-12
Site Manager, differences between, 1-2
telnet
command, 3-7
connection to router, 1-1

Terminal Interface Program (tip), B-10
TFTP, 4-14, 4-15, 5-16
tftp command, 4-14, 5-16
ti.cfg file, 2-19, 4-10
time, setting the, 8-46
timeout
  command entry, 2-14
  login, 1-11
  password, 1-11, 2-13
  Secure ID, 1-11
tip command, B-10
Transaction Program, 3-24
type command, 4-17, 5-20

U

unalias command, 9-7
underflow errors, QENET, 8-62
unmount command, 5-6
user session
  command access levels, 8-78 to 8-81
  starting manager session from within, 1-13
  terminating, 1-12
User's Login Script parameter, 2-16
user's login script, setting, 2-16

V

verbose command (for debugging aliases), 9-7
verbose option (ping command), 3-8, 3-11
VINES ping command, 3-18 to 3-20
VME routers, 4-2, 8-46
volume
  changing the active, 4-10
  displaying directory on, 4-7
  displaying the active, 4-10
  mounting, 5-4
  unmounting, 5-6

W

Welcome screen, customizing the, 1-10
wfsnmpkey command, 8-54
wfsnmpmode command, 8-53
wfsnmpseed command, 8-54
Wfterm
  accessing from Site Manager, B-18
  dialing a remote router, B-22
  file transfer functions, B-24
  initializing local modem, B-21
  logging into the Technician Interface, B-24
  modem interface settings, B-19
  opening, B-18
  overview of, B-17
  telephone call functions, B-22
wildcards, 4-2, 4-3
World Wide Web, Bay Networks home page on, xxix

X

xmodem
  command option flags, B-5
  command parameters, B-5
  command syntax, B-4
  filename conventions, B-7
  implementation notes, B-7 to B-9
  overview of, B-2
  YMODEM protocol, B-2
xmodem command, 4-13